NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

PERCEPTION OR FACT: MEASURING THE EFFECTIVENESS OF THE TERRORISM EARLY WARNING (TEW) GROUP

by

Michael Grossman

September 2005

Thesis Advisor:	Christopher Bellavita
Second Reader:	William V. Pelfrey

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2005	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Perception or Fact: Measuring the Performance of the Terrorism Early Warning (TEW) Group			**5. FUNDING NUMBERS**
6. AUTHOR(S) Michael Grossman			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

This thesis examines the structure and intelligence process of the Los Angeles Terrorism Early Warning (TEW) Group to assess its effectiveness as measured through the application of a Program Logic Model. This model verifies the links between the assumptions on which the program is based and actual program activities. It further assesses its status as a "smart practice" based on measurable criteria that are beyond perception or peer approval alone. The TEW is a regional, multi-agency and multi-disciplinary network that functions as a focal point for analyzing the strategic and operational information needed to prevent, mitigate, disrupt and respond to threats and acts of terrorism. Although efforts toward prevention are difficult to measure in any program, input and outcome are assessable. This method provides an effective means to evaluate a program while documenting what works and why. Effectiveness should not be based solely on outputs; a structure that produces them is also an indicator. The objective of this thesis is to establish a benchmark of practical standards for collaborative intelligence sharing operations that can be replicated by other regions and that will establish a common nationwide homeland security intelligence network. Based on these criteria, it is reasonable to conclude that the TEW is in fact a "smart practice." It meets its intended goals and objectives when measured according to the parameters of the Program Logic Model, and has a structured process and system that leads to preferred outcomes.

14. SUBJECT TERMS Terrorism Early Warning Group; TEW; Intelligence Fusion Center; Information Sharing;			**15. NUMBER OF PAGES** 75
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

PERCEPTION OR FACT: MEASURING THE EFFECTIVENESS OF THE TERRORISM EARLY WARNING (TEW) GROUP

Michael Grossman
Commander, Los Angeles County Sheriff's Department
B.S., California State University, Los Angeles, 1976

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
September 2005

Author: Michael Grossman

Approved by: Christopher Bellavita, Ph.D.
Thesis Advisor

William V. Pelfrey, Ph.D.
Second Reader

Douglas Porch, Ph.D.
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis examines the structure and intelligence process of the Los Angeles Terrorism Early Warning (TEW) Group to assess its effectiveness as measured through the application of a Program Logic Model. This model verifies the links between the assumptions on which the program is based and actual program activities. It further assesses its status as a "smart practice" based on measurable criteria that are beyond perception or peer approval alone. The TEW is a regional, multi-agency and multi-disciplinary network that functions as a focal point for analyzing the strategic and operational information needed to prevent, mitigate, disrupt and respond to threats and acts of terrorism. Although efforts toward prevention are difficult to measure in any program, input and outcome are assessable. This method provides an effective means to evaluate a program while documenting what works and why. Effectiveness should not be based solely on outputs; a structure that produces them is also an indicator. The objective of this thesis is to establish a benchmark of practical standards for collaborative intelligence sharing operations that can be replicated by other regions and that will establish a common nationwide homeland security intelligence network. Based on these criteria, it is reasonable to conclude that the TEW is in fact a "smart practice." It meets its intended goals and objectives when measured according to the parameters of the Program Logic Model, and has a structured process and system that leads to preferred outcomes.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

My heartfelt thanks goes to the following individuals who were always there for me throughout this incredible learning experience. To my daughter, Rachel, who is my inspiration and model for academic excellence. To my wife, Lois, for her encouragement, support and endless love that kept me motivated to achieve success. Lieutenant John Sullivan, the architect of the TEW concept, for sharing his vast knowledge of this subject with me. And, to my friend and colleague, Commander Sid Heal, for just being “Sid.”

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION / OVERVIEW

A. PROBLEM

Terrorists around the world have been active for many years, but until September 11, 2001, counter efforts within the United States were minimal. Following those attacks, however, the U.S. learned that a wide variety of issues must be addressed by a multitude of organizations and individuals to achieve the level of protection necessary to secure our homeland. Most important among these is the need for information – our first line of defense. Essential to this endeavor is the collection of information (from all sources), analysis of the information to develop actionable intelligence, and sharing of the intelligence across jurisdictional and disciplinary lines.

While the federal government continues its effort to improve the system for access to information and broader dissemination, local regions are not waiting for instructions from Washington, D.C. Many areas have already implemented initiatives to improve information sharing. The pitfall with this approach is the potential that each of these groups will be acting independently of one another and without connectivity to a larger network. A study conducted by the General Accounting Office (GAO) concluded that these efforts are not well coordinated, risk duplication of effort, and may not include all of the agencies that need access to information (GAO 2003, 11).

According to the report, a number of these individual efforts have been designated as a "best practice." However, this labeling has occurred largely by perception or self proclamation, with no formal validation. There is little evidence to substantiate the effectiveness of intelligence sharing initiatives because they currently lack specific performance measures that could determine the effectiveness of a program to meet its intended goals/objectives.

B. SIGNIFICANCE OF RESEARCH

This thesis will provide a programmatic example that can serve as a forerunner for meeting a portion of the requirements contained in Homeland Security Presidential

Directive 8 and the Interim National Preparedness Goal. On December 17, 2003, the President issued HSPD 8 to:

> …establish policies to strengthen the preparedness of the United States to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies by requiring a national domestic all-hazards preparedness goal, establishing mechanisms for improved delivery of Federal preparedness assistance to State and local governments, and outlining actions to strengthen preparedness capabilities of Federal, State, and local entities. (HSPD-8, 2003).

HSPD 8 requires the development of standards and metrics to assess capability, performance and overall preparedness of a jurisdiction or group of jurisdictions. Standards and metrics are being developed or modified in collaboration with appropriate stakeholders to measure outcomes (i.e., availability, efficiency, and effectiveness) and ensure that all elements of capability (e.g., personnel, planning, organization and leadership, equipment, training, and exercises, evaluations, and corrective actions) are considered (HSPD-8, 2003).

The Interim National Preparedness Goal establishes the national vision and priorities that will guide the efforts to strengthen the Nation's preparedness while measurable readiness benchmarks and targets are being set.

Two components of the Interim Goal are the Uniform Task List (UTL), which describes tasks that may need to be performed, and a Target Capabilities List (TCL) that details what capabilities entities will be expected to develop and maintain. There is also a requirement to include performance measures and criteria associated with each task. The TCL is comprised of 36 measures and criteria. Five of these areas, Critical Infrastructure Protection, Information Collection and Threat Recognition, Information Sharing and Collaboration, Intelligence Fusion and Analysis, and Terrorism Investigation and Intervention will be addressed in this thesis.

A description of the Los Angeles Terrorism Early Warning (TEW) Group is currently posted on the Lessons Learned Information Sharing website, LLIS.gov, which is sponsored by the U.S. Department of Homeland Security. It is currently classified as a "good story," which means that it is considered an exemplary, but not (peer) validated program. The results of the research contained in this thesis will be provided to LLIS.gov

for posting. This will serve to update the status of the TEW classification as well as provide an example of a means to comply with the requirements of HSPD-8 and the Interim National Preparedness Goal.

C. HYPOTHESIS

The objective of my thesis is to apply a process to assess the effectiveness of the Los Angeles TEW in order to validate it as a smart practice, with the intention of setting a benchmark of standards for a national model. This can be accomplished by verifying the links between the assumptions on which the program is based and actual program activities. The ultimate goal is to establish guidelines for standardized collaborative intelligence sharing operations, through the Los Angeles TEW example, that can be replicated by other regions and result in the establishment of a common nationwide network.

D. METHODLOGY

While the Los Angeles Terrorism Early Warning (TEW) Group has been in operation for eight years, the program's outcomes have never been formally measured to validate its performance expectations. This research is intended to serve as a basis for evaluating regional collaborative intelligence operations, and to establish a standard for similar programs to be measured against.

The effectiveness of the Los Angeles Terrorism Early Warning (TEW) Group will be measured through an application of a Program Logic Model (Kellogg Foundation 2001). This method of evaluation serves to clarify the links between the assumptions a program is based on, the program's actual activities, and the desired intermediate and long-term outcomes (Hass and Springer 1998, 34). The logic model can provide an understanding of what actually happens in a specific program, and it is an important tool for identifying the components needed for replication (Pumariega 1996). The Program Logic Model offers an effective means to evaluate a program while documenting what works and why.

E. SYNOPSIS OF CHAPTERS

1. Chapter I – Introduction/Overview

It is widely believed that information is the most powerful weapon we have at our disposal to combat the Global War on Terrorism (GWOT). However, without an integrated and standardized network to share that information, our nation is left only with a multitude of classic "stovepipe" operations. This lack of integration results in the opposite effect of the popular phrase "connecting the dots," and enables independent entities to possess potentially vital bits of intelligence in a vacuum. The solution lies beyond merely placing representatives from different agencies (and sometimes disciplines) together in a facility and calling it a "fusion center." There must be a standardized system to process information across jurisdictional and disciplinary boundaries. This will create a structure that can provide a template for replication in other regions that will result in the formation of a nationwide network. The opportunity to actually achieve the goal of a fully integrated intelligence fusion center is within reach, but it requires the cooperative effort of the major stakeholders in homeland security.

While a number of intelligence fusion programs have been established, there is a lack of research to validate their efficiency and effectiveness. This thesis will provide a detailed description of a model program, and through the identification and application of a performance measure evaluation tool, will validate its effectiveness and label as a "best practice."

2. Chapter II – Survey of Related Documents

This chapter explores the relevant research on information and intelligence sharing operations, primarily as evaluated by a number of commissions and government sponsored reports. These documents identify current deficiencies and desired attributes of collaborative information sharing efforts. They also look at a variety of performance measurement tools as a means to determine results and efficiency of programs. This differs from typical program evaluations that provide information on outcomes but ignore the linkage between activities and results. This chapter also contains references to studies on the evaluation of "best practices."

3. Chapter III – Methodology – The Logic Model

This chapter explores the range of approaches that exist for evaluating results management. A variety of models are identified and briefly described. The Program Logic Model is selected as the most fitting tool to apply to the information sharing process known as the Terrorism Early Warning (TEW) Group. The Program Logic Model includes specific steps to assess the full range of the program, from inputs to impact. A detailed assessment will be completed by applying the metrics of the logic model to each of the six cells of the TEW, and then to its overall integrated process

4. Chapter IV - The Terrorism Early Warning (TEW) Group

This chapter covers the history and development, and provides a detailed description of the TEW and its organizational components. It lays the foundation for understanding its purpose, process, goals and objectives, which is essential in determining if the TEW produces the expected and intended outcomes.

5. Chapter V- The Logic Model Applied to the Components of the TEW

In this chapter, each of the six cells of the TEW will be measured according to the criteria of the Program Logic Model. This includes the inputs, activities, outputs, and outcomes of each of the components as they relate to the internal TEW process.

6. Chapter VI - Performance of the TEW Model /Process

This chapter evaluates the proficiency and performance of the entire TEW process. Once each of the cells have been individually evaluated, it is essential to assess the overall program to determine its effectiveness. This will entail an assessment of all inter-cell activities in a cumulative appraisal of the phases of the logic model as it applies to the process

7. Chapter VII – Conclusion and Recommendation for Further Research

This chapter will provide a conclusion that addresses the thesis question, Perception or Fact: Does the measurement of the effectiveness of the Los Angeles Terrorism Early Warning Group validate its label as a “best practice”? Therefore, will its

replication across the nation form the type of intelligence network that is necessary to defend the nation against threats of terrorism? This chapter will also recommend further research, based on the outcome of this analysis, to measure the effectiveness of the emerging national network.

II. SURVEY OF RELATED DOCUMENTS

In order to fully assess the effectiveness of an operational program, it is necessary to look beyond references that merely describe its activities. Evaluation of the process and results is equally important, as is the ability to gain an overall perspective of homeland security issues from the national to local levels.

A thorough overview of homeland security issues is addressed in the annual reports of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (1999, 2000, and 2002) and the reports of the Markle Foundation Task Force (2002 and 2003), which essentially evaluate all aspects of our nation's readiness. These include some of the characteristics of information sharing and collaborative efforts. A third report, prepared by the General Accounting Office (GAO) for the Secretary of Homeland Security, "Homeland Security – Efforts to Improve Information Sharing Need to be Strengthened" (2003), addresses this specific issue.

In his work on the study of smart practices, Eugene Bardach suggests that, "Rarely will you have any confidence that some helpful-looking practice is actually the 'best' among all those that are addressed to the same problem. Usually, you will be looking for what, more modestly, might be called 'good' practices" (Bardach 2000, 71). He actually prefers the term "smart practice," because it has something worth analyzing that is applicable to the problem at hand.

The U.S. Department of Homeland Security's Lessons Learned Information Sharing website also addresses the issue of "best practices." It labels programs as "Lessons Learned," "Good Stories" or "Best Practices" according to the following criteria: (www.LLIS.gov).

> **Lesson Learned** is knowledge and experience—positive or negative—derived from actual incidents such as the 1995 Oklahoma City bombing and the 9/11 attacks as well as observations and historical study of operations, training, and exercises.
>
> **Good Stories** are exemplary—but non-peer-validated—initiatives implemented by various jurisdictions that have shown success in their specific environments and that may provide useful information to other communities and organizations.

> **Best Practice** is a peer-validated technique, procedure, good idea, or solution that works and is solidly grounded upon actual experience in operations, training, and exercises.
>
> **Peer-validated content:** All Lessons Learned and Best Practices are peer-validated. These resources have been conceived and developed by homeland security professionals for their peers.

These definitions refer to peer validation and successful stories that are based primarily on anecdotal information. Particularly in the "Best Practice" category, neither peer validation nor success is based on specific measurable criteria. It appears that the findings are largely based on the perception of the participants. I intend to submit the results discovered through the application of legitimate performance measures in my thesis to this website. This will serve to validate the effectiveness of the Los Angeles TEW to meet its intended goals.

In addition to government publications about information sharing efforts, the Los Angeles TEW has been mentioned in academic research. An example can be found in the NPS Thesis, "Reforming Counterintelligence in the Wake of 9/11," which states that

> ….One of the earliest and best examples in developing a counterterrorism support network that pre-dates 9/11 is the Los Angeles Terrorism Early Warning Group (TEW). To the author's knowledge there does not appear to be any historical example or case where U.S. counterintelligence functioned in such a distributed, networked and collaborative fashion (Gleghorn 2003, 83).

The TEW is based on a systems concept. The definition that best fits its model is, "a group of interacting, interrelated, or interdependent elements forming a complex whole." It is, "a condition of harmonious, orderly interaction, [and] an organized and coordinated method" (dictionary.com 2005).

Protecting our country against acts of terrorism requires an effective, integrated network for security and defense. It is the most effective means to combat the networked adversary that we now face. This has become evident from the number of violent terrorist acts that have occurred throughout the world, clearly indicating that the enemy is no longer a nation state that our military can substantially overpower.

In addition to creating a systems approach in response to this new kind of threat, the TEW was also developed as a network with a concept and structure similar to that described in *Network and Netwars: The Future of Terror, Crime and Militancy (RAND 2001).* In this, and previous work, Arquilla and Ronfeldt describe three types of networks that have become apparent in the organizational structures of netwar actors.[1] They are defined as follows and depicted in Figure 1 (RAND 2001):

> • The chain network, as in a smuggling chain where people, goods, or information move along a line of separated contacts, and where end-to-end communication must travel through the intermediate nodes.
>
> • The star, hub, or wheel network, as in a franchise or a cartel structure where a set of actors is tied to a central node or actor, and must go through that node to communicate and coordinate.
>
> • The all-channel network, as in a collaborative network of militant small groups where every group is connected to every other.

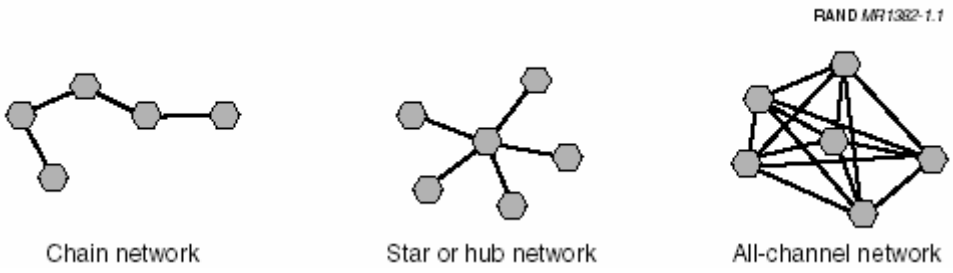

Figure 1. Three Basic Types of Networks (From RAND)

Arquilla et al suggest that no one type is exclusively used by any particular group. In fact, there are hybrids that combine two or more depending upon the intended application. These networks are not unique to "netwar" actors alone. They represent the type of arrangements that exist in the global terrorist movement in general. The application of a similar construct of the TEW enables an expanded reach of public safety intelligence collection because it allows for a deviation from the traditional bureaucratic "chain of command" that usually constrains the flow of information.

The significance of the network structure and its future impact on homeland security is best described as follows:

[1] The term netwar was coined by Arquilla and Ronfeldt in 1993 "largely because… the information revolution favored network forms of organization, doctrine, and strategy."

> The rise of networks means that power is migrating to nonstate actors, because they are able to organize into sprawling multi-organizational networks (especially "all-channel" networks, in which every node is connected to every other node) more readily than can traditional, hierarchical, state actors. This implies that conflicts will be increasingly waged by "networks," perhaps more than by "hierarchies." It also means that whoever masters the network form stands to gain the advantage (Ronfeldt and Arquilla 2001).

The GAO has looked at a number of programs and is particularly interested in the Terrorism Early Warning (TEW) Group in Los Angeles County as a potential model for coordinating regional information sharing programs. This initiative came to its attention from several sources. In 2000, the Memorial Institute for the Prevention of Terrorism (MIPT) first identified the Los Angeles TEW as a model to be replicated in other regions in the country. This was based on the Los Angeles area case study reported in the Gilmore Commission's Second Annual Report, which stated that the commission believes that:

> …the lessons learned in Los Angeles are relevant to jurisdictions nationwide and that the federal government can 1) aid in the dissemination of the lessons learned in Los Angeles; and 2) participate in educating agencies at all levels of government in the effective use of the methodologies employed in Los Angeles to draw relevant conclusions and turn them into practice (Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction [Gilmore Commission] 2000, Appendix G).

In 2002, the Department of Homeland Security's Office for Domestic Preparedness (ODP) also cited the Los Angeles TEW as a model for replication. This was based on the fact that the TEW is a full-time, multi-agency, multi-disciplinary (law, fire and health) and multi-jurisdictional (local, state and federal) operational entity that addresses all phases (pre, trans and post) of a terrorist threat or incident.

The question that remains unanswered is: does the LA TEW work? Although prevention is difficult to measure in any program, input and outcome are assessable. The aspects that need to be considered are strategic planning, performance measures and a suitable process to evaluate a collaborative program.

Strategic planning is related to outcomes. A program should have a clear mission and a vision of success. The mission outlines the organization's purpose while a vision describes how the successful organization should look (Bryson 1995, 155). This is illustrated in the federal Government Performance and Results Act of 1993 (GPRA), a traditional results management approach which requires all federal agencies to produce a strategic plan based on outcomes.

Performance measures provide a means to determine results (outcomes) and efficiency so the services or programs can be compared to their intended purpose (Hatry 1999). A range of approaches exists for evaluating results management. These include the following models: traditional, program logic, risk management, scenario-based planning, managing to standards and capabilities-based planning and assessment (Caudle 2004, 5).

An additional measurement can be accomplished by applying the evaluation tools developed to assess an actual program operation. The availability of after-action reports (AAR), which are prepared to determine the successes and failures of an event, can provide a sound resource for this purpose. The results will therefore be based on fact and not perception or a self-proclamation of success.

The self-proclamation of "best practice" comes without validation. It is therefore important to determine if minimum requirements or acceptable standards have been established for these information sharing, or fusion center operations. It would also be interesting to note if other organizations exist that are attempting similar efforts. The process to accomplish this objective is known as benchmarking (Trimble 2005, 2). It is useful for determining how like organizations are effectively accomplishing similar tasks and goals, and then comparing their achievements to those of your own operations. It is a way to look at "best practices" as a means of identifying gaps and improving performance. As the requirements for national security and the need for local intelligence are still in the developmental stages for most domestic law enforcement agencies, an ongoing benchmarking plan can still be implemented that will increase the effectiveness of the effort as it continues to evolve.

There are currently two primary sources that exist for this type of information. Much work has been done by government organizations to identify standards for fusion

center operations and best practices. The Bureau of Justice Assistance (BJA) in the Department of Justice has published a (draft) report entitled *Recommended Fusion Center Standards – Developing and Sharing Intelligence in a New World* (BJA 2005). It contains 17 items that are considered to be minimum requirements for establishing an effective fusion center operation. The Lessons Learned Information Sharing (LLIS.gov) website publication *Best Practices*: *Local Anti-Terrorism Information and Intelligence Sharing* offers several documents that contain recommendations for key elements of successful best practices, with actual examples. Both of these reports were produced with input from working groups comprised of subject matter experts from all levels of public safety agencies. The BJA report provides what is needed, while the LLIS.gov postings say how to accomplish the desired results. The TEW meets or exceeds all of the desirable traits identified in both of the documents, and was in fact specifically cited multiple times in the LLIS.gov literature as the pioneering and model operation.

Although the L.A. TEW has been labeled as a "Best Practice" by the government groups cited, there are still no standards to measure it against or to substantiate what components make up a successful system for intelligence fusion and dissemination. The ideal model will meet the needs of the nation as well as serve the local area. It is believed that the L.A. TEW is this model; however, appropriate performance measures need to be implemented to validate what is now only perception.

III. METHODOLOGY – THE LOGIC MODEL

Performance measures differ from typical program evaluations normally undertaken by government agencies, such as the GPRA process, that provide information on outcomes but little evidence on the causal linkage between activities and results. A range of approaches exists for evaluating results management. These include the following models: traditional, program logic, risk management, scenario-based planning, managing to standards, and capabilities-based planning and assessment (Caudle 2004, 5). Each of these methods has a primary objective in measuring effectiveness. For instance, the traditional model focuses on setting goals, objectives, strategies and measures, which can be used for strategic planning efforts for an organization. The program logic model describes a conversion of inputs to impacts of specific programs. The risk management model is utilized by an organization for analysis and decision making to achieve an acceptable level of risk. A scenario-based planning approach identifies possible future events and creates courses of action to address the anticipated circumstances. Managing to standards provide a way to assess achievement based on a uniform set of specifications that provide a benchmark for performance. Unfortunately, at this point in the development of our homeland security efforts, standards have yet to be established for intelligence fusion center operations such as the TEW. The last approach is the capabilities-based planning and assessment model. This process serves to identify capabilities to accomplish specific missions. This is the method that has been implemented by the U.S. Department of Homeland Security to define national preparedness goals and standards required by HSPD 8. It includes the 15 scenarios (missions) that DHS has utilized to determine what communities will need to do to be prepared and capable of responding to the identified hazards. Although this is not specifically scenario based, it has essentially combined the two approaches.

As seen with the DHS example, the methods are not mutually exclusive and can be used separately or in combination. While the scenario-based planning approach has some application for measurement of the TEW, it is limited to the response phase for course of action development for future events. This is only a portion of what the TEW does. Likewise, the scenario-based approach has limits in terms of the scope of an

anticipated event. The method of attack on September 11, 2001 was certainly not expected, therefore, preparedness for this specific type of incident was limited. The TEW is concerned with all aspects, types and phases of terrorism, from prevention to recovery. Therefore, the program logic model appears to be the most suitable for its measurement of effectiveness because it is can be tailored to be inclusive of all aspects of the intelligence fusion process. In addition, while it is difficult to measure prevention, the tangible evaluation of outcomes and impact of a program, which is not the primary focus of the other models, can certainly yield strong indications of success.

One of the most attractive attributes of using the Program Logic Model for measuring the performance of the TEW process is that it serves as a visualization tool to evaluate and improve program effectiveness at all stages. "The ability to visualize the entire scope of the problem and recognize the interconnection of seemingly disassociated factors is what empowers strategic planners with the ability to anticipate threats, determine consequence, and envisage response alternatives" (Campbell 2005). The logic model process is a tool that has been used by evaluators for many years to identify performance measures and describe the effectiveness of programs. The model and its process was provided to its grantees in the *W.K. Kellogg Foundation Evaluation Handbook* in 1998 as a means of "…facilitating thinking, planning, and communications about program objectives and actual accomplishments." This model describes logical linkages among program resources, activities, outputs, audiences, and short-, intermediate-, and long-term outcomes related to a specific problem or situation (Millar et al. 2001, 73).

The Program Logic Model includes specific steps of assessment that range from inputs to impact of a program. It is a "systematic and visual way to present and share your understanding of the relationships among the resources you have to operate your program, the activities you plan to do, and the changes or results you hope to achieve" (Kellogg Foundation 2001).

The five steps of the Program Logic Model are:

1. Inputs – the personnel, equipment and organizational resources dedicated to the program.

2. Activities – the processes, techniques and actions of the program.

3. Outputs – the direct results of the program activities (i.e., the scope of services and products delivered).

4. Outcomes – specific changes in program participant's knowledge, skills and level of functioning.

5. Impact – the changes or results that are realized from program outputs and outcomes (e.g., improved conditions, increased awareness).

When depicted as a graphic illustration, it is read from left to right, which describes the program basics over time, from planning through results. "Reading a logic model means following the chain of reasoning of "***If...then...***" statements which connect the program's parts" (Kellogg 2001). Figure 2 shows how the basic logic model is read.

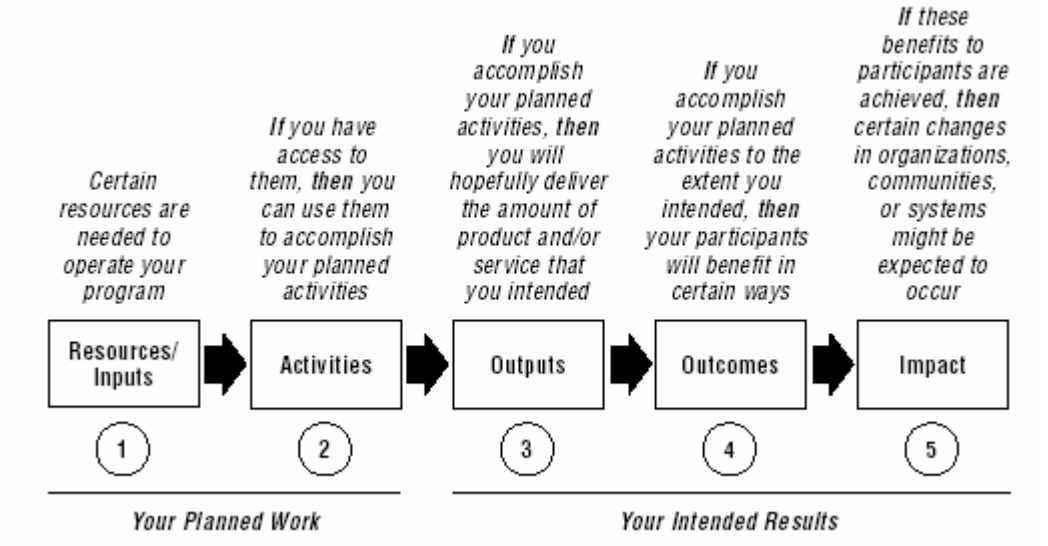

Figure 2. How to read a logic model (From Kellogg 2001)

The objective of this thesis is to dissect the TEW system and apply the process of its individual elements, or cells, into the logic model. The same evaluation will then be applied to the entire TEW. This method will serve to evaluate the interaction among its component parts and determine if the TEW meets its program goals.

The TEW is an intelligence fusion operation that is comprised of six cells that make up the "Net Assessment Group," which processes information for analysis and dissemination (outputs, outcomes and impact). These cells are briefly described as follows:[2]

1. Officer in Charge (OIC)/Command – oversees the TEW process and links with the Unified Command.[3]

2. Analysis / Synthesis – oversee intake and processing of information to and from the other cells, and develops courses of action from intelligence.

3. Consequence Management - assesses law enforcement, fire service and health consequences of events.

4. Investigative Liaison – coordinates with local, state and federal investigation and intelligence teams.

5. Epidemiological Intelligence – responsible for ongoing disease surveillance, food and water surety, agricultural threats, and coordination of disease investigations.

6. Forensic Intelligence Support – provides technical support, chemical, biological, radiological and nuclear (CBRN) reconnaissance and geospatial intelligence. Acts as liaison to subject matter experts.

The activities of each of the TEW cells will be applied to the steps of the Program Logic Model to determine if the inputs result in the desired or expected outcomes. In order to achieve a complete evaluation, the same standard must be applied to each cell of the TEW individually, and then to the overall program in a cumulative evaluation, which

[2] The entire TEW model and its functions will be described in detail in Chapter IV.

[3] Unified Command consists of the managers from multiple agencies that have the decision making authority and are in charge of an incident.

will include key inter-cell activities. Once this has been completed, the results will be compared with the After Action Report (AAR) for an actual scenario as processed by the TEW. A review of the TEW AAR for the 2000 Democratic National Convention in Los Angeles, according to the process of the program logic model, can help determine the true effectiveness of the TEW. The results of this comparison are intended to confirm the data as applied to actual incidents.

There are multiple adaptations of the logic model, and no one version is considered the best. The Kellogg manual indicates that they "come in as many sizes and shapes as the programs they represent" Their advice is, "don't hesitate to experiment with program logic model design to determine what works best for your program. And don't be concerned if your model doesn't look like one of the case examples" (Kellogg 2001). In his work, *Guidelines and Framework for Designing Basic Logic Model,* McNamara states, "Logic models can be in regard to what ever application in which the designer chooses to use them" (McNamara 2004).

With this in mind, I will adapt the traditional content of the input component of the logic model to better fit the parameters of this study. The conventional elements of input for the TEW remain consistent for the overall process and are still pertinent to producing the desired results. These are the personnel, equipment and resources necessary to accomplish all of the tasks to meet the objectives of the TEW process. The staffing includes administrative support, criminal, strategic and intelligence analysts (with multi-lingual capability), law enforcement investigators, fire service personnel, health and medical personnel (from public health and emergency medical services), and specialists in hazardous materials, explosives and forensics (criminalists). Other resources include advanced technology in computer hardware and software, communications equipment for both classified and unclassified information, and secure office space and storage for sensitive materials.

In this thesis, I will tailor the input content to describe the TEW's organizational structure as an intelligence fusion operation. Instead of physical resources as previously described, I will depict input as information, as it represents the beginning step in the TEW information analysis and synthesis process.

This thesis will address one of the questions posed in the Naval Postgraduate School paper *Homeland Security: Approaches to Results Management (*Caudle 2004), which describes a need for future research on this subject by asking the question, "Can the 'best' of these approaches be melded into a new analytical framework that can be used in an individual organization and with others who must contribute to homeland security performance? If so, what would that approach look like?"

IV THE TERRORISM EARLY WARNING (TEW) GROUP

"Let me say a word about your Terrorism Early Warning Group. It is a model for other cities and states." Secretary Tom Ridge[4]

While the vast majority of citizens failed to recognize the threat posed to our national security by terrorist acts around the globe, two deputies from the Los Angeles County Sheriff's Department were paying attention. As John Sullivan and Larry Richards observed some of the noteworthy events from 1995 to 1998, their concern grew along with the increase in global terrorism. With incidents such as the first World Trade Center bombing in New York City in 1993, the sarin gas attack in the Tokyo subway and the Oklahoma City bombing in 1995, there appeared to be an emerging trend. Then in 1996, a little known Islamist radical named Osama bin Laden issued a "fatwa" urging his followers to conduct global terrorist attacks against the United States and its citizens. The trend continued with bin Laden's affirmation of his intent to attack the United States and their interests around the world during an ABC news interview with the radical leader in May 1998, which was followed by the Khobar Towers incident in Saudi Arabia the following month.

Because terrorism comes from a complex networked threat, the traditional hierarchical military structure is largely an ineffective defense. "Combating an agile terrorist network requires an equally agile network of government agencies" (Krikorian 2004).

Information sharing and intelligence fusion centers, considered to be a necessity in the war on terrorism, are being established across the nation. The most effective of these efforts, such as the TEW model, include multi-level (local, state and federal) and

[4] Remarks by Secretary Tom Ridge to LA County first responders, April 24, 2003.

multi-disciplinary (law, fire, health and emergency management) participants who can blend all perspectives into a complete picture of threat, risk and vulnerability.

"Sullivan and Richards knew two things: that the only way to deal with a terrorist network was to create a counter-terrorism network, and that information sharing among agencies would be the key to preventing and reacting to terrorist attacks" (Pilant 2004). This method would provide the ability to facilitate both lateral and vertical unrestricted communication both within and among agencies.

The Terrorism Early Warning (TEW) Group was initiated by the Los Angeles County Sheriff's Department in 1996, to fill a void in information and knowledge about terrorism. The TEW is a multi-discipline, multi-agency and multi-jurisdictional entity with a primary mission/goal of "being the focal point for analyzing the strategic and operational information needed to combat terrorism and protect critical infrastructure" (U.S.DHS/ODP 2004). It is a regional information collection and sharing (fusion) operation that provides indications and warnings of potential terrorist threats, and operational net assessment, a process of developing course of action plans for incident response. It is based on specific information about the location and mode of attack, combined with real-time intelligence.

The original primary partners in the TEW consisted of representatives from the Los Angeles Sheriff's Department, Los Angeles Police Department, the FBI, the Los Angeles County and City Fire Departments and the Los Angeles County Health Department (public health and emergency medical services – EMS). Additional cooperating agencies included local, state and federal law enforcement, emergency management, municipal fire departments, transportation authorities, universities, airports and military (National Guard and Coast Guard).

> Initially, L.A. County's TEW aimed to develop relationships that allowed each agency to share information. The TEW's ultimate goal was to fuse different intelligence disciplines, share information, investigate emerging threats, create scenarios of different types of attacks, train to respond to those attacks, and provide tactical support to responding agencies (Pilant 2004).

Considering the size and complexity of the Los Angeles region, this would be no small task. The operational area (county) spans 4,000 square miles, contains 10 million people in 88 cities and unincorporated county areas, and has 45 local law enforcement agencies, 38 fire departments, three public health agency and 80 hospitals. It is also one of the most target rich and vulnerable areas in the nation with the ports of Long Beach and Los Angeles, the Los Angeles International Airport (LAX), the entertainment industry and a host of other commercial and industrial complexes which include aerospace, oil refineries and power plants.

> …Southern California has long had an excellent reputation for emergency response agencies that work well together, which is understandable. Earthquakes and brush fires, the two most common large-scale emergencies here, do tend to cross multiple jurisdictional lines (Bannon 2002, 30).

The question of who is in charge was settled early in the development of the TEW program. The initial participants decided that no single agency would be in control and that a unified command structure would be established. The sheriff's department agreed to act as the secretariat for the organization, which required it to provide the necessary logistics support for arranging meetings, training, communicating with the members and housing the operation.

The TEW is comprised of six integrated cells that create a system for processing incoming data through analysis by each of the cells, then synthesis of their individual evaluation to form an overall picture. The TEW is staffed by individuals and subject matter experts from law enforcement, fire and health services who work together to develop a complete picture of the current situation as well as an indication of future or potential threats. Figure 3 depicts the TEW organizational structure with an explanation of each of the cells following: (Sullivan 2005, 14)

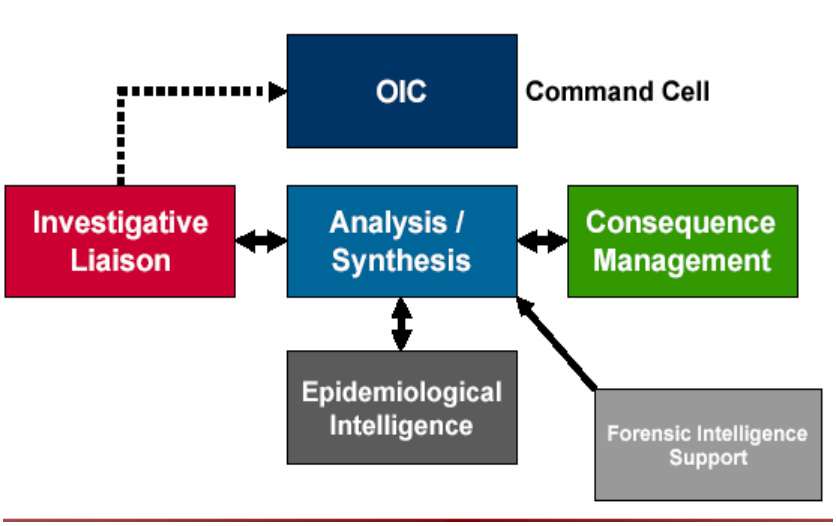

Figure 3. TEW organization (From TEW Guide 2005)

The *Officer-in-Charge (OIC) (or Unified Command)* provides command, direction and supervision, sets intelligence requirements, and is responsible for coordination with all local, state and federal agencies.

Analysis/Synthesis Cell (A/S) -- This is the central integrating hub of the TEW organization. This cell tasks out requests for information to other cells, then collects and integrates their individual products into a cohesive assessment. This process includes capturing investigative information, gathering intelligence from all sources, and analyzing and synthesizing it. The A/S cell also synchronizes information from the Investigative Liaison, Consequence Management, Epidemiological Intelligence, and the Forensic Intelligence Support/Field Assessment Support Team cells into a usable product for decision-makers. Products issued by the A/S cell include advisories, alerts, warnings, issue-specific white papers, and mission folders. Mission folders integrate threat-specific playbooks, venue-specific Response Information Folders (RIF), intelligence information, resource information, archival information on technical dimensions of threat agents, resource status, and potential course of action for incident mitigation and response.

Investigative Liaison Cell (INV-LNO) -- This cell is responsible for processing, tracking and collecting criminal and national security intelligence and leads related to terrorism. It is the primary point of contact with all classified, national and state databases, and with investigative and intelligence efforts at all levels of government. This

is the Operational Area/county link with the FBI and other intelligence and investigative entities, and the link to the national network of Joint Terrorism Task Forces (JTTF), especially the Los Angeles JTTF. The INV-LNO cell is responsible for vetting and validating leads, and assessing specific threats. It is also responsible for working with other specialized investigative entities to develop a complete intelligence picture.

Consequence Management Cell (CM) -- This cell is staffed by members of the fire service, law enforcement and medical professionals in order to assess, in the event of an attack, the current and future resource status, and to marshal specialized resources when necessary. Its members act as a technical reference, and develop potential courses of action for response to incidents involving chemical, biological, radiological, nuclear and large-scale explosives. It develops tactics and estimates logistical requirements for initiating and sustaining a comprehensive response to a terrorist attack. This cell also has the primary responsibility for developing playbooks and Response Information Folders.

Epidemiological Intelligence Cell (Epi-Intel) -- This cell integrates disease surveillance for all threats (especially biological terrorism). It facilitates the integration of public health and law enforcement investigations, provides planning estimates on the distribution of casualties and potential quarantine and treatment issues. This cell ensures the accurate and complete flow of information during intentional or suspicious outbreaks, and conducts continual monitoring for early recognition and warning of biological threats. This cell is also responsible for food and water surety and agricultural issues (including liaison to the public health community, water districts, USDA, etc.).

Forensic Intelligence Support (FIS) Cell & and Field Assessment Support Team (FAST) -- This cell is responsible for technical support, including field assessment and reconnaissance activities for CBRNE events. It supports a multi-agency response with specialized detection and sampling equipment, and provides technical assistance and specialist advice that enables law enforcement support to the fire services in the event of mass casualty/mass decontamination operations. This cell is responsible for geospatial intelligence (GEOINT), cyberterrorism issues, and "virtual reachback" to specialists at the national laboratories, military and universities. It uses this information to assess a situation and to help develop tactical courses of action. FIS/FAST uses various

technologies for modeling and simulation of the potential consequences of a terrorist event. The Field Assessment Support Team (FAST) is the field component of the FIS cell. It sends information from the field to the TEW for analysis.

A central fusion center, such as the TEW that has just been described, must not operate as an independent entity. It needs to act as a focal point for receiving, analyzing and disseminating intelligence both laterally and horizontally. Information from the field can be as vital as that from the federal or state agencies. A system that provides the vehicle to share information with all levels is therefore essential to the success of establishing that agile network of government agencies that is desired. In Los Angeles County this was accomplished through the creation of the Terrorism Liaison Officer (TLO) Program.

Shortly after the attacks of September 11, 2001, the police chiefs in the South Bay mutual aid area of Los Angeles County organized a Terrorism Advisory Group, as an effort apart from the existing TEW. One of the concepts that came out of this effort was that each agency would designate a TLO. These officers became the central point of contact for all terrorism-related information for their respective agencies. This created a pathway for information flow and coordination among the participating cities.

While this was a sound approach to establishing a network for information sharing, it had significant limitations; chief among them was that it covered a relatively small area of Los Angeles County. This meant that there was neither a formal connection to the larger geographic area, nor the ability to see the broader perspective that comes from monitoring activities and trends at the state, national or global level. Another considerable drawback was that the information sharing effort was exclusive to law enforcement.

Recognizing the extraordinary potential for the TLO Program to be an effective force-multiplier for the existing TEW, the concept was expanded countywide. The expansion was patterned after the existing mutual-aid structure, which divides the county into eight geographic areas. Each area is comprised of multiple departments with one acting as the lead agency for its area. The Los Angeles County Sheriff's Department acts as the Director of Emergency Operations and the coordinator for law enforcement mutual

aid for the operational area (county). Therefore, this existing structure proved beneficial for adapting the growing TEW network within the county.

Using the TEW as the base for an all-source fusion center, TLOs were assigned from all local law enforcement agencies, including university, railroad, airport and port police departments, as well as the 23 sheriff's stations (which provide law enforcement services for 40 cities), and specialty units (Bomb Detail, Special Enforcement Bureau/SWAT, Aero, crime lab and others). The LAPD, already a full-time partner in the TEW, was also included.

Because the TEW's multi-disciplinary approach to information sharing is vital to the success of any terrorism-related response, the TLO Program was expanded further to include representatives from the county's 38 fire departments. This included multiple TLOs from the large county and city fire departments. Representatives from the Los Angeles County Department of Health Services and the county's two other public health agencies (Pasadena and Long Beach) were also added. These representatives provide field liaison to the full-time fire and health personnel assigned to the Consequence Management and the Epidemiological Intelligence sections of the TEW. Currently, there are three health service, 50 fire and 204 law enforcement TLOs in Los Angeles County.

Consistent with the lead-agency format of the mutual aid structure, each of the eight geographic areas designated a representative to coordinate information flow between the agencies in their areas and the TEW. The fire service arm of the TLO Program was set up the same way, with representatives appointed according to its mutual aid structure.

The TLO Program has created a system for lateral and horizontal communication with law, fire and health officials, and two-way communication with the TEW. For all its seeming complexity, the process is actually quite simple: All leads come in from the field for analysis, investigation and deconfliction with multiple agencies, including the FBI, Customs, DIA, Secret Service and others. This ensures that all are aware of the investigative activities of each of the agencies and can therefore cooperate with any on-going investigations in the region. With this configuration, smaller municipal agencies,

with limited personnel and no active participation in the TEW or JTTF, can still achieve full connectivity to the information and resources available at the regional, state and federal level.

The TEW and the TLO Program transcends what was once a fragmented system of communication between local and state agencies and the federal intelligence community by acting as a regional intelligence fusion center that ensures efficient, coordinated information sharing. This structure also provides the avenue to issue advisories, alerts or warnings through the TLO network. Therefore, mass notification can be accomplished with only a single point of contact to the TEW, which effectively relieves DHS, the California Office of Homeland Security (OHS) or the JTTF from the difficult task of ensuring that local agencies are promptly notified.

The TLO Program also provides an expanded network through liaison with the private sector and the operators of critical infrastructure facilities. This is accomplished through the Homeland Security Advisory Council (HSAC), which was formed in Los Angeles and Orange counties (California State Office of Emergency Services - Region I) and is made up of CEOs of major industry. These industry executives and their respective security chiefs, who are designated as Infrastructure Liaison Officers (ILO), are linked directly to their area TLO to coordinate planning and response to terrorist-related incidents at the various facilities and locations in their jurisdiction. These relationships are facilitated primarily through subcommittee meetings of representatives from such industries as entertainment, real estate, energy and communications/media.

Few regions in the nation are as large or complex as the Los Angeles area. Many other jurisdictions throughout the country, especially the smaller cities and rural areas, neither see the need nor have the resources necessary to establish and maintain an elaborate intelligence operation like the TEW. Although major identified targets are known to be in the metropolitan areas, the terrorist network operates globally and without regard to jurisdictional boundaries. In order to have the intelligence network necessary to contend with the terrorist threat, we must be able reach out to all parts of our nation. Whether or not the operation is full-time, it should include the basic elements of the TEW

model. This will ensure that all area jurisdictions, agencies, disciplines and levels are included in the information sharing process.

One way to accomplish this is to establish state and/or regional intelligence fusion centers that operate on a full-time basis but with minimum staff. In this configuration, a full-time small scale operation, complimented by a strong TLO network (as collateral duty assignments) would be essential in order to maintain contact with the national network and keep pace with the lateral and horizontal flow of information. If a threat or incident were to occur in the region, a limited or full-scale activation could occur instantaneously with complete and current situational awareness. An effective organization of this nature would only be possible with full cooperation and prior planning among the participating agencies, followed with effective training and exercises.

Even the original TEW started as an ad hoc group of varied participants that held monthly meetings to discuss items of mutual interest and concern related to terrorism. The first of these meetings was in October 1996, and they have continued since. Representatives from the primary agencies were also activated for special events, such as the Democratic National Convention (DNC) in Los Angeles and the Y2K scare. They functioned as an operational net assessment group during these periods and then returned to their regular assignments and agencies as soon as practical. That is, until September 11, 2001.

On that fateful morning, the Undersheriff from the LASD asked the question, "What do we do?"[5] The answer was immediate. We would activate the TEW to obtain an accurate assessment of what had occurred, what we might expect, and how we should prepare. This information was then communicated to the public safety agencies and the community in the Los Angeles Region. The TEW continued to monitor the situation and events from the global, national, state and local perspective on a full-time basis to keep the executives in charge apprised of pertinent issues and intelligence information. The activation lasted at this level for the next 12 days. A dedicated full-time staff has been assigned since that time.[6]

[5] A 0645 PST phone call from Undersheriff William Stonich to (then) Captain Michael Grossman, Commander of the Emergency Operations Bureau.

[6] The Los Angeles County Board of Supervisors allocated $1.5 million for a dedicated staff that operates on a five day per week schedule with activation on an overtime basis when necessary.

As an outgrowth of the TEW, the Joint Regional Intelligence Center (JRIC) concept was developed. It brings together all of the appropriate agencies in one location, and expands the scope of operations and fully synchronizes intelligence and information sharing efforts in the Los Angeles Operational Area. The JRIC will eventually be an all-crime center with an initial emphasis on terrorist-related criminal intelligence.[7] The TEW is an embedded component that bridges criminal and operational intelligence for terrorism and emerging threats. It provides the link between the intelligence and emergency response network with connectivity to all of the law enforcement, fire and health agencies in the county via the existing mutual aid structure. Regional connectivity to the public safety community and the private sector is facilitated through the Terrorism Liaison Officer (TLO) program, the Homeland Security Advisory Council (HSAC), and Private Sector Terrorism Response Group (PSTRG) / Infrastructure Liaison Officer (ILO) initiatives.[8]

The primary partners in this endeavor are the Los Angeles County Sheriff's Department, Los Angeles Police Department, FBI Los Angeles Field Office, United States Attorney's Office for the Central District of California, and the California State Department of Justice. Numerous other federal, state and local agencies will also have representatives in the center.

Creating a compatible national intelligence network and avoiding the classic stovepipe organization is a challenge that must be met by the federal government. The FBI and the Department of Homeland Security are essential partners that need to be linked with state and regional centers. "The job of replicating the TEW model throughout the nation, thereby creating a national TEW network, has been undertaken by the United States Department of Homeland Security's Office for Domestic Preparedness (ODP). The TEW Expansion Program provides technical assistance and training, as well as expansion workshops for the prospective jurisdictions, and technical assistance and training on TEW practice" (Sullivan 2005, 4).

[7] Support for and acts of terrorism most often take the form of traditional crimes. Therefore, all crime activity should be analyzed for any nexus to terrorism (e.g. narco-terrorism).

[8] All law enforcement, fire, and health agencies in the Operational Area have a TLO representative to the TEW. The HSAC is comprised of CEO's from major corporations in Los Angeles and Orange Counties who act as senior advisors to the Sheriffs. The PSTRG/ILO program connects critical sectors of the business community to the intelligence and emergency management structure in the county.

Another aspect of the TEW Expansion Program is the establishment of the National TEW Resource Center in Los Angeles. The center provides technical assistance and training on TEW practice for prospective jurisdictions. Through this effort, ODP has essentially identified the TEW model as a benchmark which, "At its core, benchmarking aims to boost the performance by stimulating managers to match results achieved in comparable or best-performing organizations" (Schick 2001, 47). The benefit of replicating this common model is that once the TEW is in place in several locations across the country, it will ensure that the assemblage of law enforcement, fire, health and emergency management officials from appropriate local, state and federal agencies is complete. This affords the ability to share real-time information and intelligence from the perspective of all disciplines, laterally and from bottom to top and vice versa.

That being said, the integration of varied agencies, people and disciplines is relatively simple to accomplish, void, of course, of territorial, jurisdictional, cross-discipline, organizational culture, and personality issues. One of the difficulties is that it requires a paradigm shift for many involved. For instance, law enforcement traditionally acts primarily on criminal intelligence which is focused on investigation for apprehension and prosecution. While this is certainly a critical factor in the war on terrorism, it is not the only vital component to consider. The creation and maintenance of the overall picture of vulnerability, risk, criticality and threat, through the combining of criminal and strategic intelligence, is like putting a jigsaw puzzle together without knowing what the end picture is supposed to look like. The results will rarely be immediate. Bits and pieces of information (from all perspectives) are most often retrieved and shared one small piece at a time. This is not an exact science and therefore, unlike strictly criminal intelligence, the process does not produce actionable intelligence at the same rate. Sometimes it just results in more information. It is important for each of the participant components of the TEW to understand this aspect of the model so they do not have unreasonable expectations of its purpose or become disenchanted because there may be no immediate results or return on their investment.

It is essential however, to stay informed and current with all available information, especially focusing on any indications of potential impact to the region. In order to understand the importance of keeping pace with an ongoing situational

awareness, it is helpful to be familiar with a theory related to the speed of the decision cycle. This is particularly significant if a response to a perceived threat or actual attack becomes necessary. Boyd's Cycle is a series of "time competitive, Observation-Orientation-Decision-Action (OODA) cycles," (Heal 2000, 73) that exist during conflict.[9] It starts with an observation of the status of the adversary and self, and then looks at the perspective of the overall situation (orientation). From this information a decision is made which "takes into account all of the factors present at the time of the orientation" (Heal 2000, 74). The last phase is to carry out the decision by taking action. The cycle then repeats itself throughout an incident as circumstances evolve. The opponent who can go through the cycle fastest gains the tactical or strategic advantage. Without having adequate and current information, it is difficult to make an informed decision in a time of conflict.

This knowledge can prove to be crucial when incident commanders are provided with actionable intelligence because they will recognize what they have and be prepared to take quick and appropriate action. Otherwise, they will always trail the tempo of the adversary and be forced to start from the beginning in each episode of conflict.

The TEW is exceptional at monitoring all aspects of global information relative to terrorism, and functioning as the focal point for fusion and sharing of information for the Los Angeles region. It is especially effective during the operational net assessment mode in linking real-time information with strategy and emergency response. Because of its capacity to maintain a constant situational awareness, the ability to prevent, mitigate, disrupt or respond to threats and acts of terrorism is enhanced.

[9] The OODA Loop is a creation of Colonel John Boyd, USAF (Ret).

V. THE LOGIC MODEL APPLIED TO THE COMPONENTS OF THE TEW

Now that the TEW model has been explained in detail, a comprehensive look at each of its cells will depict how the logic model has been applied in order to illustrate the process and the intended results. In essence, this is a detailed look at the components of the system, and establishment of the network on which the formation of the TEW was based.[10]

A. OFFICER IN CHARGE (OIC) CELL

It is the ultimate goal of this cell to ensure that the TEW provides effective on-going decision support (information) to agency executives, incident commander(s) (in the event of an actual incident) and other users. In other words, an information fusion process which results in actionable intelligence to address all phases of the terrorist threat. The International Association of Chief's of Police (IACP) addressed this issue, saying that prevention is paramount in any homeland security strategy. However, "to date the vast majority of federal homeland security efforts have focused on increasing our national capabilities to respond to and recover from a terrorist attack" (IACP 2005, 3). While the shift from response to prevention has been long in coming in the national strategy, the TEW was founded on this premise. It is the responsibility of the OIC cell to ensure that prevention remains the primary goal.

The OIC Cell (Figure 4) coordinates the overall TEW process with input from agency executives and incident commander(s), to determine their (commander's) intent and any specific standing intelligence requirements they may have. This includes any public order issues that arise, as well as the ongoing duty to report critical information if it is determined that a threat exists which would require input from the executives to establish specific requirements. A Commander's Critical Intelligence Requirement (CCIR), and Requests for Information (RFI), would also be considered as input to the OIC Cell that starts the intelligence process. This might come in the form of a question such as, is there a threat to the Tournament of Roses Parade?

[10] Lt. John Sullivan in a series of discussions with author from January - July 2005, unpublished data.

It is the responsibility of the OIC to articulate the commander's intent and adjust the process and organization as needed to meet any specific situation. The middle managers from the primary agencies that staff this function are to stimulate problem solving and monitor intelligence dynamics to prevent mirror imaging,[11] group thinking or tunnel vision. They are tasked with assuring quality control and obtaining final approval of the results produced for dissemination in the process phase.

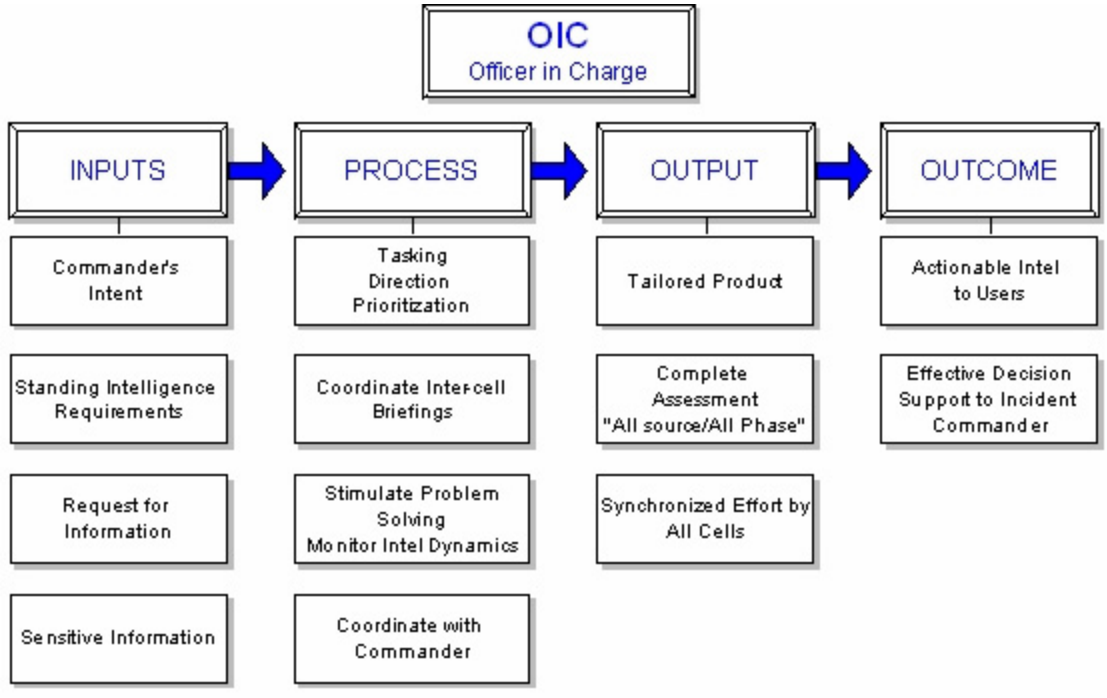

Figure 4. Officer in Charge Cell

B. ANALYSIS SYNTHESIS CELL

This cell is the focal point for coordination of information and interaction with all of the other cells of the TEW. It takes input from all available sources, including the OIC's intent and tasking, leads, reports and RFIs, classified and Open Source Intelligence (OSINT) and inputs from other cells and TEWs. All of the information is prioritized as Priority Intelligence Requirements (PIR), Other Intelligence Requirements (OIR) or Specific Intelligence Requirements (SIR).

[11] Mirror imaging in intelligence analysis is to believe that an adversary thinks the same way as you or your group.

The process consists of OSINT exploitation, vetting and validating leads, tasking other cells with specific requirements, and a net assessment or evaluation of the results (synthesis). It is responsible for monitoring of trends and potential activities that provide indications of what, where, when and how a terrorist incident may occur, and issuing the appropriate notification (outputs) in the form of advisories, alerts or warnings. This is known in the intelligence community as Indications and Warning (I&W). One of the most important aspects of this process is the fusion of Operational Intelligence (OPINT), the everyday information from the field or world around us that has been analyzed, and Criminal Intelligence (CRMINT), the information specific to criminal investigations. It also combines strategic and tactical information in order to provide a complete threat picture (Figure 5).

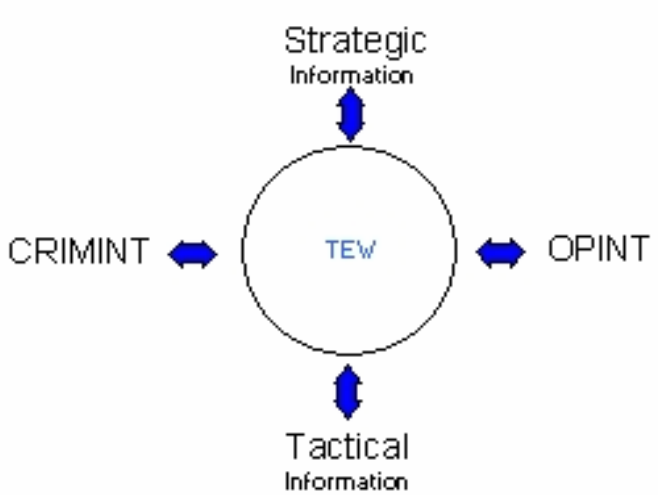

Figure 5. Intelligence Fusion

The blending or fusion of all these diverse aspects in the synthesis phase of the TEW process is the significant factor that separates the TEW model from other intelligence fusion operations that rely only on criminal information and intelligence as indicators of potential terrorist intentions or activities. This bridges the operational net assessment process with the Indications and Warning (I&W) function. The final outcome of this effort results in the ability to identify trends and potentials, capabilities and intentions of an adversary and a complete situational awareness within the TEW. The activities and expected results of the Analysis/Synthesis Cell are depicted in Figure 6.

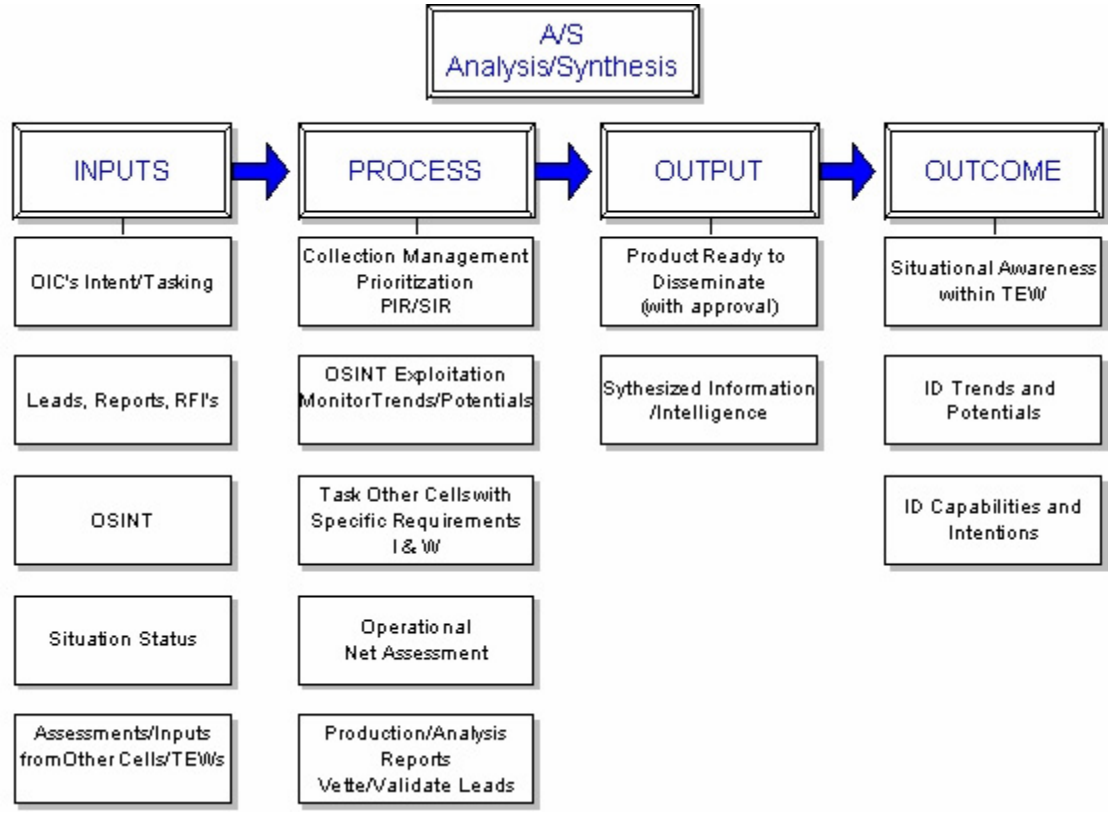

Figure 6. Analysis/Synthesis Cell

C. CONSEQUENCE MANAGEMENT CELL

The Consequence Management Cell (Figure 7) is staffed primarily by fire and EMS personnel. In addition to their disciplinary requirements on operational issues, they are responsible for coordinating the fire and EMS component of the TLO program.

Once all of the pertinent information is obtained, this cell is responsible for the development (pre-event) and use (trans- and post-event) of playbooks and Response Information Folders (RIF).[12] The playbooks contain information for responding to specific classes and types of threats, including chemical, biological, radiological, nuclear and explosive (CBRNE). The standardized Response Information Folders include terrain awareness tools such as location maps, lists of resources and available infrastructure for dealing with an attack on a specific site or system. The combination of these two, along with real-time information, are contained in a Mission Folder which provides crises

[12] Response Information Folders (RIF) were originally identified as target folders. The nomenclature was changed due to the negative connotation of "target" to many commercial establishments.

management plans and recommended responses (course of action). The Mission Folder is a unique situation specific tool that gives timely guidance to an incident commander during an actual event.

This cell provides context to the other cells (output) to understand the potential impact of the myriad types of potential terrorist attacks. It also forecasts and documents what is needed (logistics) and who is appropriate and capable of handling the job. While infrastructure protection is commonly focused on vulnerability and criticality (impact) assessment, it must also be linked with knowledge of what the threat is in order to get a complete picture of the risk and potential terrorist targeting. Understanding vulnerabilities and potential target sites is the part of the overall intelligence picture that is provided by the Consequence Management Cell. This is one component of the process of integrating the inputs and products of the entire TEW intelligence process, which is known as “Intelligence Preparation for Operations” (IPO). The end result is a thorough understanding of what might be faced, what is needed to handle the situation and what changes might be needed to meet new demands.

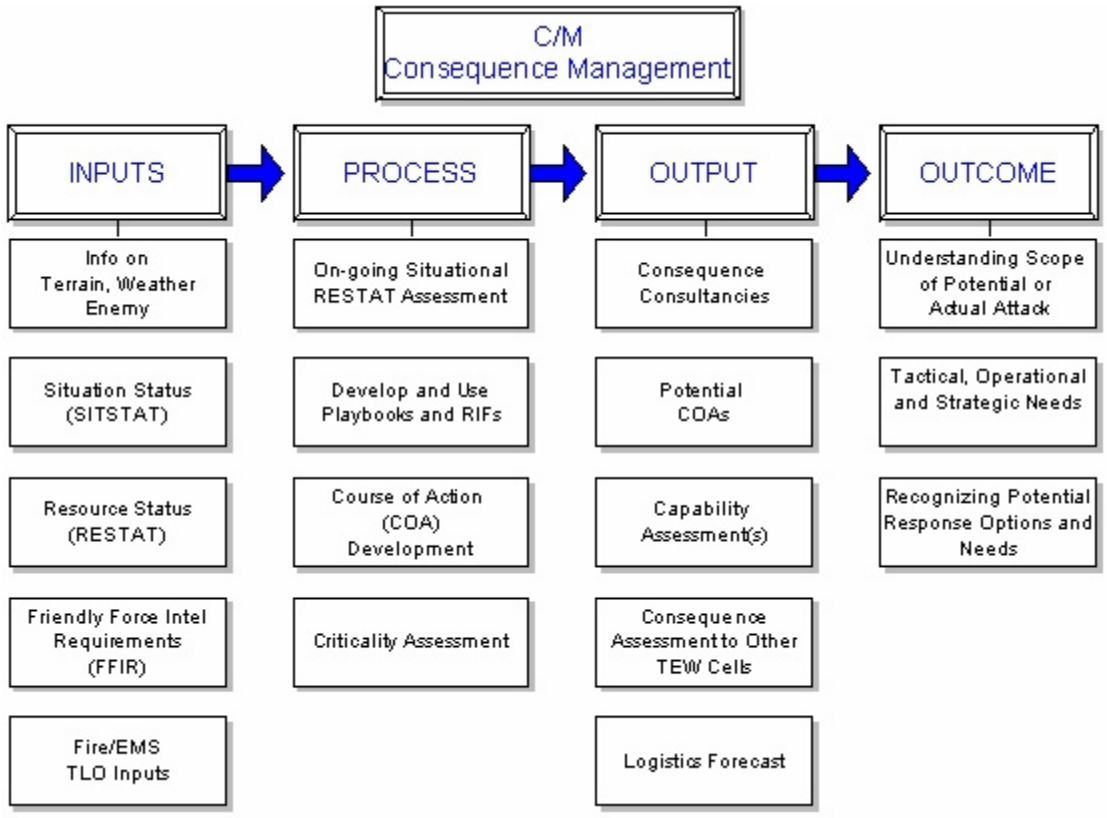

Figure 7. Consequence Management Cell

D. INVESTIGATIVE LIAISON CELL

This cell (Figure 8) coordinates the law TLO component and manages the integration of the overall TLO and ILO private sector programs. The personnel assigned to this function are responsible for source development, nurturing relationships and maintaining ongoing liaison with all information sources and investigative agencies to access criminal intelligence.

Sensitive (classified) information is provided (output) directly to the OIC as appropriate for situational awareness and decision support. Feedback (result of input) is communicated back to the investigative partners. This cell also imparts the criminal context to the other cells, and relates a cumulative picture of individual (criminal) actions to the overall situation and their link to ongoing criminal conspiracies or social movements. One example is showing the relationship between what appears to be isolated criminal acts, such as trademark violations and counterfeiting, and providing financial support to known terrorist groups.

The end goal (outcome) of this cell is to establish and communicate the link between criminal activity and investigations and the TEW process, or the CRIMINT component as previously depicted in Figure 5.

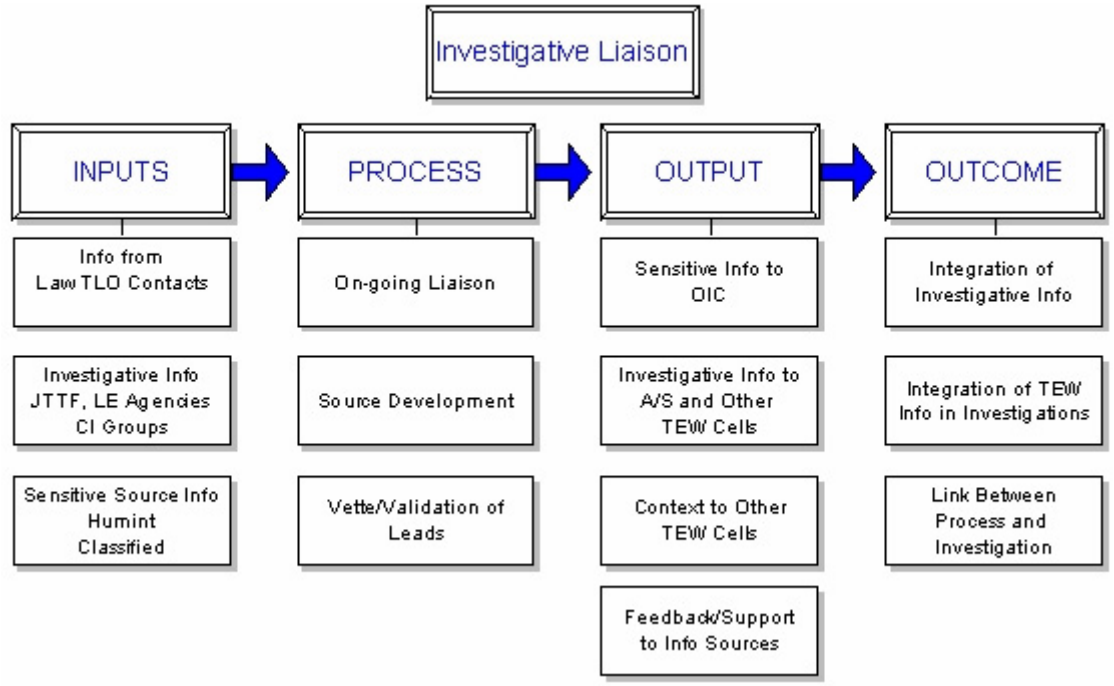

Figure 8. Investigative Liaison Cell

E. EPIDEMIOLOGICAL INTELLIGENCE CELL

The EPI Intel Cell (Figure 9) is staffed by public health and EMS medical staff.[13] They monitor epidemiological information from a wide range of medical, agricultural, veterinary and other open sources (inputs). This cell is also responsible for coordination of the health TLO program.

By exploring all available medical and public health information, personnel in this cell will be able to project the sequence, potential impact, necessary resources and the best course of action to recommend to the incident commander(s). In the event that a bio-attack occurs, the first signs of its existence would most likely be discovered through this process.

[13] The EPI Intel Cell EMS staff is comprised of medical personnel (nurses and MDs) as opposed to the first responder EMS (fire personnel) that staff the Consequence Management Cell.

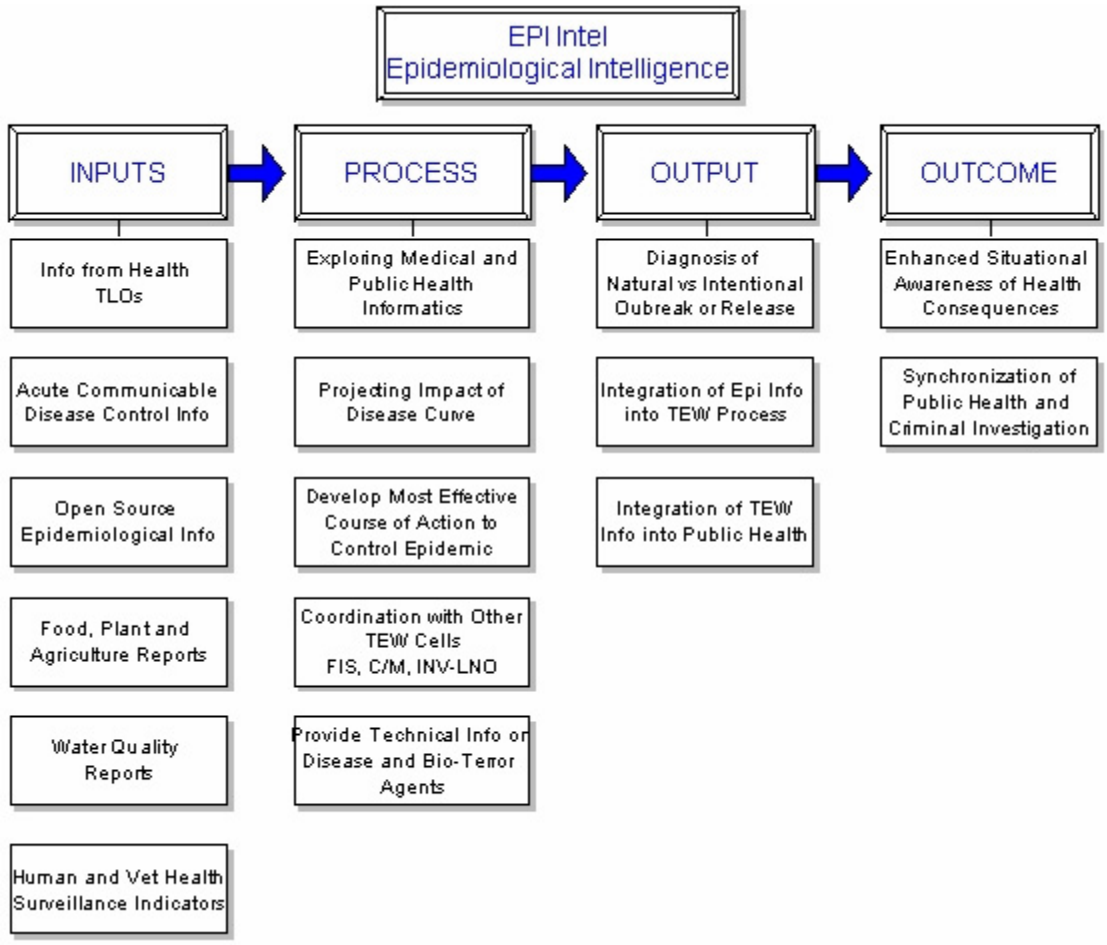

Figure 9. Epidemiological Intelligence Cell

F. FORENSIC INTELLIGENCE SUPPORT CELL

The FIS Cell (figure 10) obtains its data (input) from technical means such as video, overhead and aerial images (geospatial intelligence), meteorological (weather) data, advanced computer tools (cyber intelligence) and detectors and sensors (e.g. dosimeters and radiological pagers) to determine the presence of CBRN substances. Its personnel exploit this data (process) to infuse the information into the TEW intelligence process in order to better understand and quantify technical aspects of what is occurring. They convert highly technical information and data into understandable terms, and determine the potential impact of what might happen, which facilitates course of action development. A great deal of technical knowledge is required, hence the need for virtual reachback to subject matter experts, who would not likely be on staff.

This practice results in the translation of complex technical data into graphic products (output) for easy understanding of a situation in order to facilitate decision making. This may include bar graphs, plume modeling and visual maps with multiple layers of data.

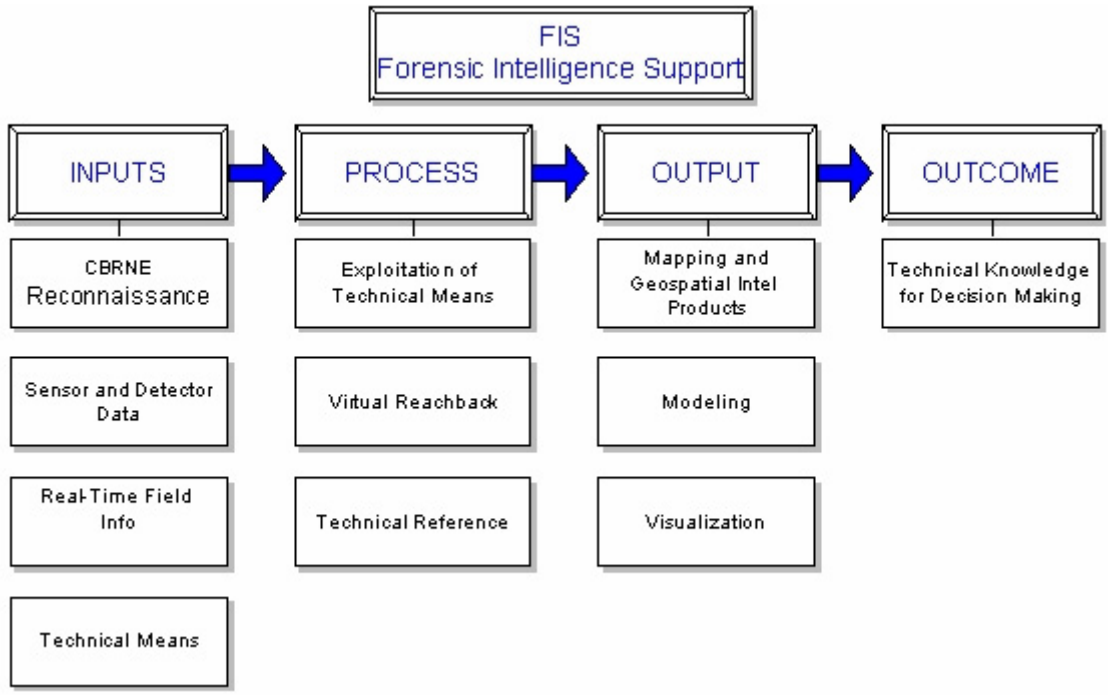

Figure 10. Forensic Intelligence Support Cell

THIS PAGE INTENTIONALLY LEFT BLANK

VI. PERFORMANCE MEASURES OF THE TEW MODEL

With a thorough understanding of the system's components, the following information will apply the logic model to the overall process of intelligence fusion and analysis. It will describe how the TEW model functions as a networked operation, and establish standards and metrics to assess the system's capability. This will also demonstrate how it incorporates the "Best" or "Smart Practice" attributes of intelligence fusion operations as required in HSPD 8 and the Interim National Preparedness Goal.

A. THE TEW INTELLIGENCE PROCESS

The TEW provides a system for fusing information from multiple disciplines and sources through all phases of an event to determine the overall picture (i.e. all-source-all-phase fusion).The process (Figure 11) starts with input of raw data (not assessed) and information requirements from the multi-disciplinary decision and policy makers. They determine what information is critical and necessary in order to formulate appropriate decisions for the circumstances. Requirements will change through different phases of an event. For example, in the prevention mode, this may include general questions such as: Do we face the threat of terrorism in the United States or in our region, and what can be done about it? The answer may then lead to the next question: Do we need to expand our anti-terrorism effort over the next five years? The nature of these questions will be more specific when an event is eminent or has already occurred.

The process phase can be described as an analysis that can determine an indication of what, when, how or where terrorist activity may occur, and produce the appropriate warning (Indications and Warning, I&W). This "operational net assessment" provides all of the information that is known at a given point in time and that is related to a threat and our capacity to deal with it.

The vast amount of incoming data must first be examined for its validity. Individual actions that could signify criminal or terrorist activity (transactions) and actions consistent with terrorist Tactics, Techniques and Procedures (TTPs) should be

identified (signature).[14] Analysts should also be looking for any patterns of activity occurring over time that appear as developing or existing trends. From this information it is possible to forecast potential terrorist actions (trends and potentials). It is also important to gauge the adversary's capability of carrying out any threat and to determine what the intention or objective may be.

Another component of the process phase is the assessment of threat, vulnerability and criticality, which is equivalent to the level of risk to the geographic area of operation. Using all of the information available, an assessment is then conducted from a multi-disciplinary perspective, in order to match the risk with local capabilities.

Decision support products (output) in the form of briefings, advisories, alerts and warnings, in addition to the mission folders which include Response Information Folders and playbooks, are provided as situation awareness tools for decision makers and field operations personnel. In the event of a terrorist attack, a common operating picture of what is actually happening (in real-time) at the location(s) of the incidents facilitates the development of appropriate courses of action. In other words, this provides the information to describe the existing situation with recommendations of what to do about it.

The ability to anticipate emerging or current threats and provide effective decision support through actionable intelligence (that has been disseminated to the end user) are the desired outcome of the TEW process. The systematic analysis from a multi-disciplinary perspective for all phases of terrorism is what sets the TEW model apart from other intelligence fusion operations. The impact of this practice results in the effective prevention, mitigation, disruption, response and recovery to threats and acts of terrorism.[15]

[14] An explanation of the terms transaction and signature as depicted in Figure 11.

[15] Lt. John Sullivan in a series of discussions with author from January - July 2005, unpublished data.

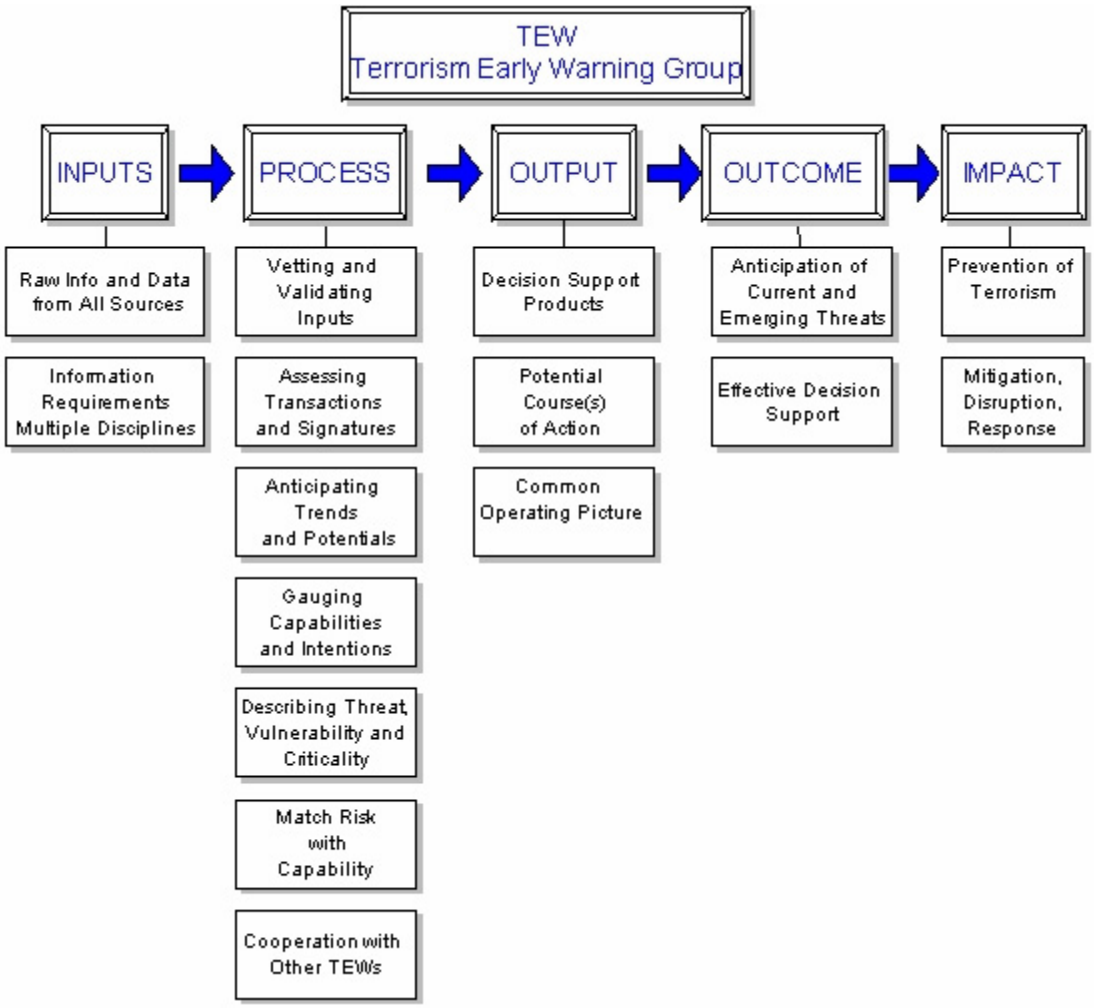

Figure 11. The TEW Process Model

B. THE PRIMARY EXAMPLE – 2000 DEMOCRATIC NATIONAL CONVENTION

Since its inception in 1996, the TEW has participated in numerous training and exercise drills which include internal programs, the annual Los Angeles County-wide exercise and the National Westwind 99 exercise.[16] In addition, the TEW was instrumental in the efficient handling of the anthrax hoaxes that occurred in Los Angeles in 1998 and again in 2001. This was the subject of Congressional testimony before the House Committee on Government Reform, Subcommittee on Government Efficiency,

[16] Westwind 99 simulated a chemical attack on a local air show by a fictional domestic terrorist group, resulting in the simulated deaths of 2,000 victims. The exercise encompassed the pre-investigation phase, detecting the possibility of a terrorist attack, a comprehensive consequence management response, an investigative response, and culminated in the arrest of the perpetrators.

Financial Management and Intergovernmental Relations, by the Assistant Director in Charge of the Los Angeles Division FBI, in which he stated (in part):

> The effectiveness of the TEW was put to the test during the last quarter of 1998, when the Southern California region experienced over 40 anthrax hoax threats. Early in that period, those incidents garnered a high level of media attention and incurred a cost to the public averaging $600,000 per response. By the end of that period, the participating agencies had cut response costs dramatically, lowered the media profile, and reduced the unnecessary decontamination of victims. Both the events of September 11th and the actual dissemination of anthrax spores that took place shortly thereafter, resulted in the handling of several hundred anthrax-related calls and incidents by the FBILA and its regional partners. The preceding years of interagency cooperation had already established the basis for consistent protocols in the handling of anthrax-related calls by the TEW member agencies bearing that responsibility. (Iden 2002)

In the 1998 anthrax hoaxes, the TEW demonstrated its ability to anticipate threats, recognize real-time information and coordinate the development and implementation of long-term policy and training needs. As incidents began to occur in Wichita, Kansas and to move across the country, the TEW identified the anthrax trend, which activated pre-planning efforts for addressing similar potential incidents in the Los Angeles region. After discussions on the issue among the TEW members at their monthly meetings, from August – December, an advisory was formulated entitled *Responding to Potential Weapons of Mass Destruction (WMD) and Anthrax Threat Incidents.* This was disseminated to all of the field units of the participating law enforcement, fire and health agencies in the region.

In December 1998, after seven incidents occurred in the area in only 10 days, representatives of the six primary agencies[17] met to develop formal policy and procedures. The outcome was a structured set of indicators that provided the means to assess the need to respond, or not, and that resulted in the conservation of vital resources and funds. Within hours of the meeting, interdepartmental bulletins were issued defining protocol, polices and procedures for handling anthrax-related calls (Gilmore Commission 2000).

[17] LASD, LAPD, LAFD, LACoFD, L.A. Co Department of Health Services (DHS) and the FBI.

When the anthrax hoaxes again surfaced in 2001, the primary TEW participants, with the addition of representatives from the police and fire departments from the independent cities, assembled to update the protocol, which had not been changed since its inception in 1998. The revised document was widely distributed to all of the public safety agencies and hospitals in the county.

The most comprehensive example of an activation of the TEW for an actual operation is the Democratic National Convention (DNC) which was held in Los Angeles, California from August 7 – 18, 2000. During this short period the TEW demonstrated its capability to integrate field intelligence from multiple sources to form an overall countywide picture. It provided an intelligence fusion system that integrated criminal and operational intelligence with emergency management practices across jurisdictional lines.

For the purpose of this paper, the DNC will serve as a proxy for evaluation, since a major terrorist incident has not occurred in Los Angeles. It was a comprehensive event that replicated many of the same tasks that would be necessary to deal with a complex terrorist incident, and that required the same kind of information collection, processing and decision support that would be essential in the event of a terrorist incident in Southern California.

The Democratic National Convention, held at the Staples Center in downtown Los Angeles, expected to draw 5,000 delegates and nearly 20,000 media personnel. Due to its significance and participation by the President of the United States and numerous elected and high ranking government officials, it was designated as a National Security Special Event (NSSE).[18] The Los Angeles Police and Fire Departments were the agencies with primary responsibility for the law enforcement, fire suppression, hazardous materials and EMS response.

In addition to the DNC, the Reform Party's National Convention was also held during this period (August 10 – 13, 2000) at the convention center in the City of Long Beach, which is also within the County of Los Angeles Operational Area. The Long

[18] A National Special Security Event (NSSE) requires the U.S. Secret Service to assume the role as the lead agency for the design and implementation of the operational security plan (PDD-62 1998).

Beach Police and Fire Departments had the same primary responsibilities as those mentioned for the DNC in the City of Los Angeles.

Because of the large number of individuals attending the conventions, delegates and dignitaries were housed in locations throughout the county area. Local police, fire and EMS were the primary agencies responsible for the sites and for managing any incidents that occurred within their jurisdictions. The Los Angeles County Sheriff's Department had responsibility for coordinating law enforcement mutual aid in the event that additional resources became necessary to respond to any unusual occurrence or civil disorder. According to the state's Standardized Emergency Management System (SEMS), any requests for assistance necessary beyond the L.A. Operational Area were to be routed through the County Emergency Operations Center (CEOC) to the California State Office of Emergency Services (OES).

A wide variety of groups had indicated their intent to protest during the convention on both national and international controversial causes. A number of the groups and individual participants, who had recently been involved in unlawful demonstrations at events in Canada, Seattle and Washington D.C., were expected to be in Los Angeles. They would undoubtedly take full advantage of the opportunity for exposure that would be afforded through the extensive media coverage of these events. Their actions would potentially include mass disruption through the use of unconventional tactics and weapons, mostly directed at law enforcement, at multiple locations and jurisdictions throughout the county. Another concern was the possibility of hoax attacks, which could be equally disruptive and taxing to available resources.

The mission of the TEW was to monitor and assess all events throughout the county that could have the potential to impact public order or the special events themselves. While other agencies were concerned only with the venues and problems posed by events in their jurisdiction, the TEW was observing and evaluating the bigger picture to identify trends, potentials and indicators of what, where and how acts of disruption might occur. This afforded the necessary information to assess the overall situation in order to match the risk with local capabilities, and act to prevent, mitigate,

disrupt or coordinate a response if necessary. The TEW also acted as a clearinghouse for vetting incidents and investigative leads, as well as a central operation for rumor control.

At the same time, the LAPD maintained an intelligence operations center to support its mobile field forces. The United States Secret Service (USSS) activated a Multi Agency Coordination Center (MACC), and the FBI operated a Joint Operations Center (JOC). All of these efforts continued for the duration of the DNC, and were primarily focused on tactical issues. The TEW took a more strategic approach by monitoring all of the activities in the entire county operational area and assessing whether they posed a threat to the main event. This was accomplished by receiving inputs from the other intelligence centers, Mobile Field Forces (MFF), patrol units, fire units, sensitive (classified) reporting, open source information and mass media. This data was then analyzed according to the TEW process, turned into such products as briefings for command staff and advisories on TTPs which were issued to field personnel from all of the participating agencies including the LASD (MFF and jail teams), FBI, LAPD, USSS, CHP and L.A. City Fire.

The value of the TEW was demonstrated on numerous occasions during this period. As an example, an incident occurred that was first believed to be an intentional contamination of fuel that had been delivered to multiple law enforcement agencies, disabling numerous police cars and motorcycles. After a thorough investigation by a combination of multiple TEW cells and testing of the substance by the Forensic Intelligence Support element, it was determined that a trailer containing waste oil had accidentally been mixed with gasoline and then dispatched by the oil company. The driver, who had been arrested, was subsequently released once the facts were determined.

The next example depicts how the TEW process functioned from input to impact for a particular situation. The TEW received information (input) that law enforcement officers patrolling the neighborhood adjacent to the Staples Center found several piles of large rocks that had been carefully placed near trees marked with red paint. Apparently the protestors planned to use the rocks against law enforcement during the demonstrations, and the red marks were pre-placed so the protestors could easily locate the rocks. This information and all other similar data about protestor’s tactics that had

been obtained by the TEW was assessed (process), and turned into an advisory (output) issued to all law enforcement patrol units and MFFs on the demonstrators tactics. As a result of the advisory, the protestors were essentially disarmed (outcome) and this type of attack was no longer available to the adversary (impact). These are only two of many such incidents that were processed by the TEW, which essentially took raw information and produced actionable intelligence. The result was that all field forces were afforded the ability to act on data that they otherwise may not have known.

Depending upon the nature of a particular threat or incident, there may be occasion when individual TEW cells do not appear to have active participation in the process. As an example, although there were no biological or public health issues that surfaced during this operational period, the Epidemiological Intelligence Cell maintained contact with the Centers for Disease Control (CDC) and conducted enhanced disease surveillance for early detection of any unusual occurrence or outbreak. Similarly, there was a continual evaluation for chemical, biological or radiological substances, as well as the development of response requirements to deal with their consequences.

In other words, the entire TEW organization actively participated in the process so that all aspects of the event were considered in order to maintain a current situational awareness and the ability to act and respond appropriately.

The purpose of this paper up until this point has been to describe how the TEW's concept could be applied to the adapted version of the Program Logic Model. The example of the DNC activation now provides an opportunity to assess the TEW's application for actual performance, according to the same measures of the logic model. The intent is to determine if the logic model works for this application, and if the TEW is effective based on this criterion. It will both describe and measure its performance and ability to meet its intended goals under actual conditions (Figure 12). It should be noted here that because of the sensitive nature of some information, specific details will intentionally be withheld.

As previously described, the evaluation process of the logic model begins with inputs, which in the case of the TEW includes the intelligence requirements as delineated by the incident commander. The objective of the member agencies during the operational

period of the DNC was to utilize the TEW fusion model to collect and analyze all available information, provide comprehensive situational awareness, produce actionable intelligence, and develop course of action recommendations across jurisdictional lines for all participating agencies and disciplines.[19] Other inputs consisted of information obtained from advanced technology, such as chemical, biological and radiological detection devices, visualization tools (geospatial mapping), virtual planning software (plume modeling), and aircraft (fixed wing and helicopters), which provided aerial imagery. The majority of information was obtained from open source intelligence, which is available on the Internet and through the mass media. Some intelligence was also obtained via sensitive (classified) reporting. Field reconnaissance and observation in the form of investigative leads and countywide incident reporting from the myriad of law enforcement and fire agencies in the field was also a major source. The key information obtained included the number of demonstrators, their movement or activity, their location(s), who they were or what group they may have been associated with, when the information was received (currency), and what special equipment or weapons they possessed. This information, regardless of the source, was recorded in a SALUTE[20] report that provided a uniform format for analysis of the groups' Tactics, Techniques and Procedures (TTP). In the case of the DNC for instance, participants included known militant groups such as "Anarchists" and "Black Block," which are prone to violent tactics against law enforcement.

The process consisted of continuously integrating all inputs to analyze the TTPs of those who intended to disrupt the event(s). Again, in the case of the DNC, the analysis looked at the adversary's vulnerabilities, crowd movement, formation, leadership and other indications that might reveal intentions or specific tactics. This phase also included a continual analysis of all available information collected from all sources throughout the county for indications of potential impact to the event(s).

---

[19] The principal participating agencies were, LASD, LAPD, LAFD, LACoFD, L.A. Co Department of Health Services (DHS), FBILA, LBPD and as needed to all other law enforcement and fire departments in the L.A. Operational Area that could be activated under mutual aid agreements.

[20] SALUTE stands for the categories of the report to record and evaluate the Size, Activity, Location, Uniform, Time and Equipment of each lead or incident.

As a result of processing the available intelligence, a series of TEW advisories (outputs) on TTPs were produced in real-time and issued directly to the field commanders from the several participating agencies. These described potential issues with logistics, special weapons, mass arrest, counter law enforcement operations and disruptive techniques. For example, field forces and mobile booking teams were advised to be alert that protestors intended to use super glue on their hands to impede the booking process and obscure their fingerprints. Potential course of action recommendations for prevention, resolution and disruption of the specific situations were also included. In addition, current intelligence reports/summaries and a complete Mission Folder containing playbooks and a *digital* Response Information Folder for the Staples Center were provided to the primary agencies.[21] This effort was undertaken to augment the information included in the original operations plans of the various agencies. It provided an ongoing understanding of an evolving and dynamic situation and changing threat potential. Because the plans developed by the LAPD, FBI and USSS were specifically for the NSSE venue, the TEW was the only entity to consider other areas of interest in the county, and to analyze the tactics of the opposing force, develop potential courses of action for future operations, and evaluate overhead imagery from outside the primary event. The TEW was the only overarching organization that worked to integrate all of the efforts into one common operational picture.

The primary outcome achieved from the implementation of the TEW process during this event was that public safety participants and policy and decision makers had a comprehensive understanding and common operating picture of the existing situation. They had the ability to quickly determine the most viable course of action for the given circumstances. Because field commanders knew what to expect from the hard-core demonstrators at the convention site, they were able to readily identify negative actions and intervene accordingly to diminish the capability of the "Anarchists." Public order and safety was maintained and the convention proceedings were not disrupted. The public was protected and lawful citizens were able to participate in peaceful demonstrations.

[21] This digital version of the RIF for Staples Center (not included in original operations plans) was developed by the TEW, in collaboration with the Lawrence Livermore National Laboratory, and shared with the primary agencies which included the LAPD, FBI and USSS.

The impact realized from the joint effort influenced by the TEW process was that civil disobedience was prevented from occurring, and the right to free speech was protected. Ultimately, the preservation of the political process was achieved without incident.

In addition to validating the TEW process according to the Program Logic Model, the anthrax and DNC examples are intended to demonstrate the existence of a structure for effective information sharing in the Los Angeles region. While numerous investigative leads and smaller incidents have been dealt with since then, no other event had the complexity to drive all of the elements of the TEW process. Although the majority of these lesser incidents did not provide a great deal of actionable information, some definitely attracted our attention. For example, in testimony given before the Senate Committee on Homeland Security and Governmental Affairs, it was stated that in many of the Intellectual Property Rights (IPR) crimes committed in Los Angeles, "There are mounting indicators of the involvement of terrorist groups and their supporters" (Stedman 2005). Specific examples of evidence were provided confirming that these high profit-generating crimes were committed by supporters of known terrorist groups or by those who had connections to them. At one crime scene, deputies observed numerous Hezbollah flags and a photo of its leader, Hassan Nasrallah. In another case, one of the suspects taken into custody displayed a tattoo of the Hezbollah flag on his arm. This type of information provides input to the TEW process for strategic analysis as well as actionable criminal information for the FBI's Joint Terrorism Task Force (JTTF).

While the TEW provides the organization to integrate efforts and fuse data, it is not the one decisive factor in achieving the goal of preventing terrorism. Many other agencies are linked to the TEW operation, which forms the local network structure that is essential for the co-production of intelligence. The advantage of this strategy is that not every node of the network needs to be equal in size to add value, it is only important that each is connected to the system to make it whole. The significance of the TEW is that absent its functioning as the initiator and coordinator of this network, this integration would not likely occur.

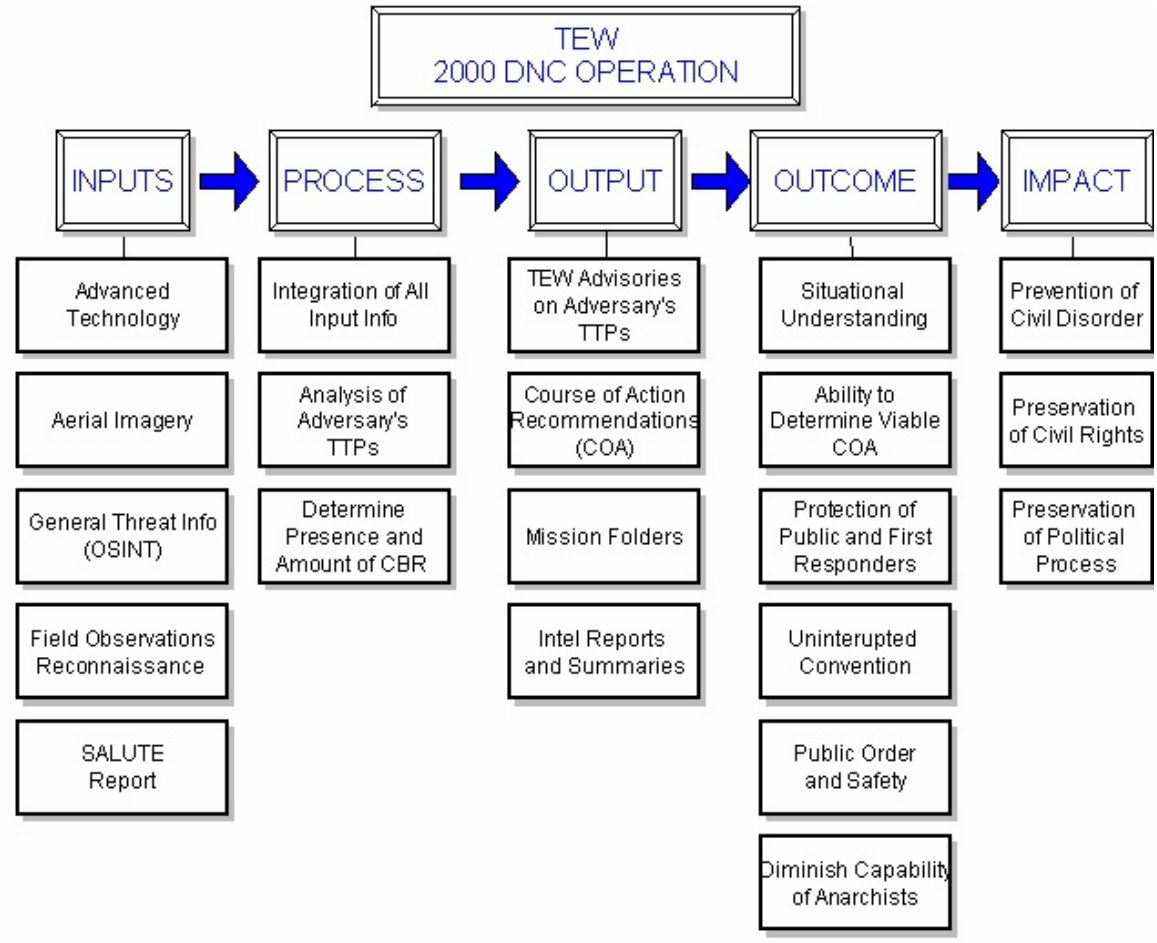

Figure 12. TEW DNC Example Operation

VII. SUMMARY / CONCLUSION

A. SUMMARY

Although efforts toward prevention are difficult to measure in any program, input and outcome are assessable. The purpose of measuring the performance of the TEW using the Program Logic Model was to conduct a self-assessment of its ability to meet its intended goals. The evaluation was not meant to be a comparison against other information sharing and intelligence fusion center operations, or to make a determination of which is better or "best." It did, however, verify that the TEW program successfully meets its intended goals and objectives of being the focal point at the operational level for effectively analyzing the strategic and operational information needed to combat terrorism and protect critical infrastructure. One of its most significant merits is that it reaches beyond the one dimensional aspect of criminal intelligence to include the operational considerations of all jurisdictions, levels and disciplines. The effectiveness of the TEW model was then evaluated by applying the logic model through a retrospective look at its performance during an actual event as represented by the 2000 Democratic National Convention. The results showed that the process was also effective when utilized in real-time situations and not just when evaluated conceptually.

The initial intent of this thesis was to validate the TEW as a "best practice." However, lacking official requirements or standards, it is virtually impossible to determine what a "best practice" actually looks like or how to measure its performance. At any rate, we should not be competing amongst ourselves to see who is "best" when our ultimate goal is to collectively be smarter and faster than our adversary. It was discovered that a more realistic approach considers what constitutes a "smart practice," because "it has something worth analyzing that is applicable to the problem at hand" (Bardach 2000, 71).

The solution to achieving effective intelligence sharing for homeland security lies beyond merely placing representatives from different agencies (and sometimes disciplines) together in facilities across the nation and calling them "fusion centers." There must be a standardized system to effectively process information across

jurisdictional and disciplinary boundaries, like the organizational structure illustrated in the DNC example, and that can be replicated in each of these centers. They should then be linked to one another, forming the type of network that is necessary to defend against an agile enemy. The need for this structure can not be underestimated. It is essential to our national security because we have learned that, "…whoever masters the network form stands to gain the advantage" (Ronfeldt and Arquilla 2001).

In his paper on *Measuring Prevention*, Woodbury makes several points that are pertinent to this study. For instance, he says, "Defining the 'what' to measure is where we are challenged" (Woodbury 2005). Because it is often difficult to show results for prevention efforts, final outcomes may not always be the best way to measure effectiveness. "*The process and systems that lead to preferred outcomes* [emphasis mine] are measured when ultimate outcome measurement is impossible." (Woodbury 2005). The existence of a collaborative system that "enables and promotes the integration and analysis of data from all sources" is in itself a form of measurement. Accordingly, four measurable desired outcomes or goals for an organizational effort to prevent terrorist attacks can be based on the following: (Woodbury 2005)

- Increased ability to identify indications of an existing or future threat.
- Increased ability to evaluate the potential of threats as they are identified.
- Reduced vulnerability of critical infrastructures and other potential targets.
- Increased appropriateness of protection and/or other threat response activities.

Based on these criteria, not just perception or peer approval, it would be reasonable to conclude that the TEW is in fact a "smart practice." It meets its intended goals and objectives when measured according to the parameters of the Program Logic Model, and it contains the "process and systems that lead to preferred outcomes." In addition, the TEW model addresses the following target capabilities which are listed as desired traits in the National Preparedness Guidance section of HSPD 8:

- Information Collection and Threat Detection
- Intelligence Fusion and Analysis

- Information Sharing and Collaboration
- Terrorism Investigation and Apprehension
- CBRNE Detection
- Risk Analysis
- Critical Infrastructure Protection
- Food/Agriculture Safety and Defense
- Public Health Epidemiological Investigation and Testing

The venture to create a compatible national homeland security intelligence network, based on the TEW model, has already been initiated by the Los Angeles Sheriff's Department. This effort has been supported by the U.S. Department of Homeland Security's Office for Domestic Preparedness (ODP) through the establishment of the National TEW Resource Center in Los Angeles. The TEW Expansion Program provides technical assistance and training, as well as expansion workshops for the prospective jurisdictions, and technical assistance and training on TEW practice" (Sullivan 2005, 4). The goal of this program is to expand the TEW model to at least 51 major urban areas across the nation.

Because the TEW model has essentially established practical standards for intelligence fusion center operations, which includes all of the appropriate disciplines and jurisdictions that need access to information, the duplication of effort and regional centers acting independently without connectivity to the larger network can be avoided. The 2003 GAO report, *Homeland Security: Efforts to Improve Information Sharing Need to be Strengthened,* cites these points as essential in order to achieve a well coordinated national homeland security network.

B. RECOMMENDATION FOR FURTHER RESEARCH

There is still much to be learned in this emerging field of intelligence for local public safety agencies. This research has validated the effectiveness of the TEW to meet its goals and objectives at the local level, and has become a benchmark of measurable attributes for the assessment of like programs. Further research is necessary to determine how to actually develop the network to repeat L.A.'s success in individual nodes and then apply the concept across the entire network. Once this is underway, the same performance measures should be applied to the additional TEW operations as they come

on line. This will be necessary to determine if they are also achieving their intended goals, and that the process remains consistent with the other nodes of the emerging network. The same measures should later be applied to the overall distributed national network in order to measure its effectiveness and capacity for the co-production of intelligence.

A final thought: When the Joint Regional Intelligence Center (JRIC) matures into an all-crimes analysis operation, will the intelligence process implemented by the TEW prove to be as effective when applied to threats other than international and domestic terrorism? Could this particular system possibly lead to a more efficient way to enhance the safety and security of our neighborhoods in dealing with crime prevention and law enforcement issues such as the terror caused by gang violence?

LIST OF REFERENCES

Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction [Gilmore Commission]. 2002. *Fourth Annual Report to the President and the Congress: Implementing the National Strategy*. Washington D.C.

_____, 2000. *Second Annual Report to the President and the Congress: Toward a National Strategy for Combating Terrorism.* Washington D.C.

_____, 1999. *First Annual Report to the President and the Congress: Assessing the Threat.* Washington D.C.

Arquilla, John and David Ronfeldt. 2001. *Networks and Netwars: The Future of Terror, Crime and Militancy Chapter one: The Advent of Netwar (revisited).* RAND.

Bannon, Anne L. 2002. "California Teaming." *Homeland Security Professional:* November/December.

Bardach, Eugene. 2000. Part III "'Smart (Best) Practices'" Research: Understanding and Making Use of What Look Like Good Ideas from Somewhere Else." In *A Practical Guide for Policy Analysis*. New York: Chatham House.

Bryson, J. M. 1995. *Strategic Planning for Public and Nonprofit Organizations.* Rev. ed. San Francisco: Jossey-Bass.

Campbell, Harold G. 2005. Logic Models in Support of Homeland Security Strategy Development. *Journal of Homeland Security and Emergency Management:* Vol 2, Issue 2, Article 9.

Caudle, Sharon. 2004. *Homeland Security: Approaches to Results Management.* Center for Homeland Defense and Security, Naval Postgraduate School, Monterey, CA: Unpublished paper.

Gleghorn, Todd E. 2003. *Exposing the Seams: The Impetus for Reforming U.S. Counterintelligence.* Master's Thesis. Naval Postgraduate School, Monterey, CA.

Hass, P.J. and J.F. Springer. 1998. *Applied Policy Research: Concepts and Cases.* New York: Garland.

Hatry, H. P. 1999. “What Types of Performance Information Should be Tracked?” In *Performance Measurement: Getting Results*. Washington D.C.: Urban Institute Press.

Heal, Charles"Sid". 2000. Chapter 7: Strategy and Tactics. In *Sound Doctrine: A Tactical Primer*. New York: Lantern Books.

International Association of Chiefs of Police (IACP). “From Hometown Security to Homeland Security.” Alexandria, VA, [cited June 1, 2005]. Available from http://www.theiacp.org/leg_policy/HomelandSecurtityWP.PDF.

Krikorian, Greg. 2004. “Terrorism Early Warning Group Works to Keep L.A.'s Guard Up.” *Los Angeles Times* B, November 7.

Lessons Learned Information Sharing (LLIS.gov). “Best Practice: Local Anti-Terrorism Information and Intelligence Sharing Overview.” 2004 [cited May 20 2005]. Available from https://llis.dhs.gov/member/secure/index.cfm.

Lessons Learned Information Sharing Website (LLIS.gov). [cited July 16, 2004]. Available from https://llis.dhs.gov/member/secure/index.cfm.

Markle Foundation Task Force. “Creating a Trusted Information Network for Homeland Security.” 2003 [cited July 20, 2004]. Available from http://www.markletaskforce.org/Report2_Part_One.pdf.

_____. “Protecting America's Freedom in the Information Age.” 2002 [cited July 20 2004]. Available from http://www.markletaskforce.org/documents/Markle_Report_Part1.pdf.

McNamara, Carter. “Guidelines and Framework for Designing Basic Logic Model.” [cited August 14, 2004]. Available from http://www.mapnp.org/library/np_progs/np_mod/org_frm.htm.

Millar, A., R.S. Simeone and J.T. Carnevale. 2001. *Logic Models: A Systems Tool for Performance Management, Evaluation and Program Planning.*

Office of the President of the United States. March 31, 2005. *Interim National Preparedness Goal Homeland Security Presidential Directive 8: National Preparedness.* Washington D.C.

Pilant, Lois. May 2004. “Strategic Modeling: Los Angeles County's Counter-Terrorism Program is Being Duplicated Nationwide.” *Police Magazine:* Vol. 28. Torrance, CA: Bobit Publications.

Presidential Decision Directive PDD-62 (1998). *National Special Security Events (NSSE). in U.S. Secret Service* [database online]. [cited July 15, 2005]. Available from http://www.secretservice.gov/nsse.shtml.

Pumariega, A. J. 1996. Culturally Competent Outcome Evaluation in Systems of Care for Children's Mental Health. *Journal of Child and Family Studies* 5, 389-393.

Ronfeldt, David and John Arquilla. 2001. “Networks, Netwars, and the Fight for the Future.” *First Monday: Peer Reviewed Journal on the Internet* Vol 6, no. Number 10.

Schick, Allen. 2001. *Getting Performance Measures to Measure Up QUICKER, BETTER, CHEAPER? Managing Performance in American Government, ed.* Rockefeller Institute Press.

Sullivan, John P. 2005. *Los Angeles County Terrorism Early Warning Group Implementation Guide (Draft).* Manual ed. Vol. 1. Los Angeles, CA.

Terrorism Early Warning Group. 2000. *After Action Report, Democratic National Convention (DNC).* Los Angeles, CA, Unpublished.

Testimony of: Iden, Ronald L. Assistant Director in Charge, Los Angeles Division, FBI. March 28, 2002. *"Bio Terrorism."* Edited by Committee on Government Reform, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations.

Testimony of: Stedman, John C. Lieutenant, Los Angeles Sheriff’s Department. May 25, 2005. “*Counterfeit Goods: Easy Cash for Criminals and Terrorists.”* United States Senate, Committee on Homeland Security and Governmental Affairs.

Trimble, Dave. Benchmarking - Uncovering Best Practices and Learning from Others. in BPR Online Learning Center [database online]. 2005 [cited May 20 Available from http://www.prosci.com/benchmarking.htm.

U.S. Department of Homeland Security, Office for Domestic Preparedness (ODP). 2004. *Terrorism Early Warning Group, Intelligence Coordination Between Federal, State and Local Agencies.*

U.S. Department of Justice, Bureau of Justice Assistance (BJA). May 2005. *Recommended Fusion Center Standards, Developing and Sharing Intelligence in a New World (Draft).*Global Justice Information Sharing Initiative. Washington D.C.

U.S. General Accounting Office. 2003. *Homeland Security: Efforts to Improve Information Sharing Need to Be Strengthened. Report to the Secretary of Homeland Security.* Vol. GAO-03-760. Washington D.C.

Woodbury, Glen L. 2005. *Measuring Performance* (draft). Monterey CA: Center for Homeland Defense and Security, Naval Postgraduate School.

W.K. Kellogg Foundation. Using Logic Models to Bring Together Evaluation and Action: Logic Model Development Guide. Battle Creek, Michigan, [cited July 16, 2004]. Available from http://www.wkkf.org/Pubs/Tools/Evaluation/Pub3669.pdf.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Leroy D. Baca, Sheriff
   Los Angeles Sheriff's Department
   Monterey Park, California

4. William Moore
   Lessons Learned Information Sharing - LLIS.gov
   Department of Homeland Security
   Washington D.C

5. Rep. Jane Harman
   Member of Congress 36th District, California
   Washington D.C.

6. Lt. John Sullivan
   National TEW Resource Center
   Los Angeles, California

7. Christopher Bellavita
   Naval Postgraduate School
   Department of National Security Affairs
   Monterey, California

8. William V. Pelfrey
   Naval Postgraduate School
   Department of National Security Affairs
   Monterey, California